Snap Server® Administrator Guide

GuardianOS v2.4

for Snap Servers 4200/4400/4500/14000

SnapAppliance™

COPYRIGHT

TRADEMARKS

REVISIONS

Part Number: 70980590-003 Rev A

END USER LICENSE AGREEMENT (EULA)

FOR USE OF SNAP APPLIANCE STORAGE SOLUTIONS AND RELATED INSTALLATION UTILITIES

SNAP IP, ASSIST, AND NASMANAGER ("INSTALLATION UTILITIES"); THE SYSTEM SOFTWARE EMBEDDED IN THE SNAP SERVER STORAGE SOLUTION ("EMBEDDED SOFTWARE"); SOFTWARE MARKETED BY SNAP APPLIANCE OR THAT IS EMBEDDED IN OR OTHERWISE CONSTITUTES A PART OF SNAP APPLIANCE COMPUTER HARDWARE PRODUCT(S) (SOMETIMES REFERRED TO COLLECTIVELY HEREIN, TOGETHER WITH THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE, AS THE "LICENSED SOFTWARE"), EXCEPT WHERE EXPRESSLY PROVIDED OTHERWISE, ARE PROPRIETARY COMPUTER SOFTWARE BELONGING TO SNAP APPLIANCE, INC. OR ITS LICENSORS. UNITED STATES COPYRIGHT AND OTHER FEDERAL AND STATE LAWS AND INTERNATIONAL LAWS AND TREATIES PROTECT THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE.

USE OF THE SNAP SERVER STORAGE SOLUTION ("SERVER") OR THE INSTALLATION UTILITIES IMPLIES YOUR AGREEMENT TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. BY USING THE INSTALLATION UTILITIES OR THE SERVER, YOU ARE ENTERING INTO A BINDING CONTRACT WITH SNAP APPLIANCE, INC.. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE INSTALLATION UTILITIES, THE EMBEDDED SOFTWARE, OR THE SERVER AND SHOULD PROMPTLY RETURN THIS ENTIRE PACKAGE, INCLUDING THE INSTALLATION UTILITIES AND SERVER, TO THE PLACE WHERE YOU PURCHASED IT FOR A FULL REFUND.

1. Ownership and Copyright. The Installation Utilities and Embedded Software are licensed, not sold to you, for use only as permitted by the terms and conditions of this Agreement. Snap Appliance reserves any rights not expressly granted to you. The Licensed Software is composed of multiple, separately written and copyrighted modular software programs. Various Licensed Software programs (the "Public Software") are copyrighted and made available under the GNU General Public License or other licenses that permit copying, modification and redistribution of source code (which licenses are referred to as "Public Licenses").

The Public Software is licensed pursuant to (i) the terms of the applicable Public License located in the related software source code file(s), and/or in its on-line documentation; and (ii) to the extent allowable under the applicable Public License. The source code is available at oss.snapappliance.com. To receive a copy of the GNU General Public License, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Various Public Software programs are copyrighted by the Regents of the University of California and are derived from material licensed to the University of California by its contributors, to which the following disclaimer applies:

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

All other Licensed Software programs (the "Restricted Software") are copyrighted by Snap Appliance or its licensors and are licensed pursuant to all of the terms of this Agreement.

Copying of the Licensed Software, unless specifically authorized in writing by Snap Appliance, is prohibited by law. You may not use, copy, modify, sell, lease, sublease, or otherwise transfer the Installation Utilities or Embedded Software, or any copy or modification, in whole or in part, except as expressly provided in this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE ONLY (ARTICLES 2 - 7):

2. License. In consideration of the premises of this License Agreement, your payment of any applicable license fee for Restricted Software, and/or your purchase of a Snap Appliance Server that the Licensed Software accompanies, for the term of intellectual property protection inhering in the Licensed Software, Snap Appliance hereby grants to you a limited, personal, and non-exclusive license to install and execute ("Use") the Restricted Software solely under the terms and conditions of this Agreement and only on the Server in connection with which Snap Appliance originally provided such Restricted Software. You are given a non-exclusive license to use the Installation Utilities and Embedded Software in conjunction with a Server, make one copy of the Installation Utilities for archival and backup purposes only, and/or transfer your Server and copies of the Installation Utilities and the accompanying documentation to a third party provided that you provide Snap Appliance written notice of the transfer within 30 days after the transfer date and you do not retain any copy of the transferred software. Any such transferee's rights and obligations with respect to the transferred software and documentation are as set forth in this Agreement.

3. Reproduction of Proprietary Notices. You may not sublicense, distribute, rent, lease, lend, or otherwise convey the Restricted Software or any portion thereof to anyone, and under no circumstance may you use or allow the use of the Restricted Software in any manner other than as expressly set forth herein. Copies of the Installation Utilities must be labeled with the Snap Appliance copyright notice and other proprietary legends found on the original media.

4. Protection of Trade Secrets. The Licensed Software contains trade secrets, and in order to protect them, you agree that you will not reverse assemble, decompile or disassemble, or otherwise reverse engineer any portion of the Restricted Software, or permit others to do so, except as permitted by applicable law, but then only to the extent that Snap Appliance (and/or its licensors) is not legally entitled to exclude or limit such rights by contract. Except with respect to online documentation copied for backup or archival purposes, you may not copy any documentation pertaining to the Licensed Software. You agree that your use and possession of the Licensed Software is permitted only in accordance with the terms and conditions of this Agreement.

5. Ownership of Restricted Software. You agree and acknowledge that, (i) Snap Appliance transfers no ownership interest in the Restricted Software, in the intellectual property in any Restricted Software or in any Restricted Software copy, to you under this Agreement or otherwise, (ii) Snap Appliance and its licensors reserve all rights not expressly granted to you hereunder, and (iii) the Restricted Software is protected by United States Copyright Law and international treaties relating to protection of copyright, and other intellectual property protection laws of the U.S. and other countries.

6. Termination. If you fail to fulfill any of your material obligations under this Agreement, Snap Appliance and/or its licensors may pursue all available legal remedies to enforce this Agreement, and Snap Appliance may, at any time after your default of this Agreement, terminate this Agreement and all licenses and rights granted to you hereunder. You agree that any Snap Appliance suppliers referenced in the Restricted Software are third-party beneficiaries of this Agreement, and may enforce this Agreement as it relates to their intellectual property. You further agree that, if Snap Appliance terminates this Agreement for your default, you will, within thirty (30) days after any such termination, deliver to Snap Appliance or render unusable all Restricted Software originally provided to you hereunder and any copies thereof embodied in any medium.

7. Government End Users. The Installation Utilities, Embedded Software, and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202, Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, and FAR Section 12.212, and successor provisions thereof, as applicable. Any use modification, reproduction release, performance, display, or disclosure of the Installation Utilities or Embedded Software and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except as expressly permitted by the terms of this Agreement.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE AND, SUBJECT TO SECTION 1, TO PUBLIC SOFTWARE (ARTICLES 8 - 15):

8. Export Laws. Notwithstanding any provision of any Public License to the contrary, Snap Appliance shall have no duty to deliver or otherwise furnish source code of any Public Software if it cannot establish to its reasonable satisfaction that such delivery or furnishing will not violate applicable US laws and regulations. You hereby assure that you will not export or re-export any Licensed Software except in full compliance with all applicable laws, regulations, executive orders, and the like pertaining to export and/or re-export, including without limitation USA versions of the same. No Licensed Software may be exported or re-exported into (or to a national or resident of) any country to which the U.S. embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. You agree to ascertain necessary licensing procedures and obtain required licenses before exporting or re-exporting either. You also agree to indemnify Snap Appliance and assume all financial responsibility for any losses it may suffer if you do not comply with this paragraph.

9. Disclaimer of Warranties. THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE ARE LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND. SNAP APPLIANCE HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, RELATING TO THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

10. Limitation of Liability. IN NO EVENT WILL SNAP APPLIANCE OR ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT EXCEED THE PRICE THAT YOU PAID FOR THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE. FURTHERMORE, IN NO EVENT WILL SNAP APPLIANCE OR ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS, LOST DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR PUNITIVE DAMAGES ARISING OUT OF OR UNDER THIS AGREEMENT OR THE APPLICABLE PUBLIC LICENSE. The limitation of liability set forth in this paragraph will apply whether or not Snap Appliance or its licensor was advised of the possibility of the loss, liability, or damages and notwithstanding any failure of essential purpose of any limited remedy. Since some states do not allow exclusions or limitations of liability for consequential or incidental damages, this provision may not apply to you.

11. Waiver. No delay or failure of Snap Appliance to exercise any right under this Agreement, nor any partial exercise thereof, shall be deemed to constitute a waiver of any rights granted hereunder or at law.

12. Unlawful Provision(s). If any provision of the Agreement is held to be unenforceable for any reason, all other provisions of this Agreement shall nevertheless be deemed valid and enforceable to the fullest extent possible.

13. Applicable Law. Except with respect to any Public Software program for which the applicable Public License contains provisions expressly stating the applicable governing law (with respect to which the law so specified shall govern all aspects of such agreement, including the provisions incorporated into such Public License hereunder), the terms of this Agreement (including, to the extent allowable under the Public License, all software governed by a Public License which does not specify a governing law) will be governed by the laws of the State of California, without reference to its choice of law rules, and the United States, including U.S. Copyright laws.

14. Entire Agreement. This Agreement and all applicable Public Licenses supersede all proposals, negotiations, conversations, discussions, all other agreements, oral or written, and all past course of dealing between you and Snap Appliance relating to the Licensed Software or the terms of its license to you, and may only be modified in writing signed by you and Snap Appliance.

15. Contractor/Manufacturer. Snap Appliance, Inc., 2001 Logic Drive, San Jose, CA 95124, USA

COMPUTER ASSOCIATES INTERNATIONAL, INC. ("CA")

ETRUST ANTIVIRUS

END USER LIMITED LICENSE AGREEMENT (THE "AGREEMENT")

CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS REGARDING YOUR USE OF ETRUST ANTIVIRUS, INCLUDING ITS CODE AND DOCUMENTATION (THE "PROGRAM") BEFOREUSING THE PROGRAM.

1. CA PROVIDES YOU WITH ONE COPY OF THE PROGRAM AND LICENSES THE PROGRAM TO YOU PURSUANT TO THE TERMS OF THIS AGREEMENT.

- **a.** The Program is provided solely for your nonexclusive, limited use for a single user and a single CPU for your internal data processing purposes. You may not transfer the Program to another CPU or site or upgrade the CPU without the payment of CA's applicable fees. You may NOT exceed this usage limitation.
- **b.** If the Program is a beta program and not generally available to date, CA does not guarantee that the generally available release will be identical to the beta program or that the generally available release will not require reinstallation. You agree that if otherwise required by CA, you shall provide CA with specific information concerning your experiences with the operation of the Program.
- **c.** If the Program is an evaluation version, you agree to use the Program solely for evaluation purposes, in accordance with usage restrictions set forth in Section 1(a), for the thirty-day evaluation period. At the end of the evaluation period, you agree to return to CA all copies or partial copies of the Program or certify to CA that all copies or partial copies of the Program have been destroyed from your computer libraries and/or storage devices. You agree and acknowledge that the evaluation version of the Program will not operate after the expiration of the evaluation period.
- **d.** You may copy the Program solely for backup or archival purposes. The Program is a trade secret of CA and confidential information of CA and its licensors. You agree to keep the Program strictly confidential and not to disclose the Program nor allow anyone to have access to the Program other than your authorized employees. Title to the Program and all changes, modifications and derivative works thereto shall remain with CA and its licensors. The Program is protected by copyright, patent, trademark and other laws and international treaties.

2. Without the prior written consent of CA, you may not:

- **a.** (a) transfer, assign, use, copy, distribute or modify the Program, in whole or in part, except as expressly permitted in this Agreement;
- **b.** (b) decompile, reverse assemble or otherwise reverse engineer the Program, except as expressly permitted under applicable law;
- **c.** (c) remove or alter any of the copyright notices or other proprietary markings on any copies of the Program; or
- **d.** (d) perform, publish or release benchmarks or other comparisons of the Program without CA's prior written consent.

3. CA may immediately terminate this Agreement in the event of any failure to comply with any of the above terms. Such termination shall be in addition to and not in lieu of any criminal, civil or other remedies available to CA.

4. CA DOES NOT WARRANT THAT THE PROGRAM WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAM WILL BE UNINTERRUPTED, ERROR FREE OR WILL APPEAR AS DESCRIBED IN THE DOCUMENTATION.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW: (A) THE PROGRAM IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND; (B) CA AND ITS LICENSORS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (C) IN NO EVENT WILL CA OR ITS LICENSORS BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, INCLUDING TIME, MONEY, GOODWILL AND ANY INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM EVEN IF CA HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

5. You acknowledge that the Program is provided with "Restricted Rights" as set forth in 48 C.F.R. Sec. 12.212, 48 C.F.R. Sec. 52.227-19(c)(1) and (2) or DFARS Sec. 252.227.7013(c)(1)(ii) or such applicable successor provisions. CA is the manufacturer of the Program. This Agreement shall be construed according to and governed by the laws of the State of New York. You are required to observe the relevant US Export Administration Regulations and other applicable regulations. Outside the United States, no product support services, if available, will be offered by CA without a proof of purchase or license from an authorized source. Snap Appliance

ANY QUESTIONS CONCERNING THIS AGREEMENT SHOULD BE REFERRED TO COMPUTER ASSOCIATES INTERNATIONAL, INC., ONE COMPUTER ASSOCIATES PLAZA, ISLANDIA, NY 11749.

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND THAT YOU ACCEPT ITS TERMS AND CONDITIONS. YOU ALSO AGREE THAT THIS AGREEMENT CONSTITUTES THE COMPLETE AGREEMENT BETWEEN US REGARDING THIS SUBJECT MATTER AND THAT IT SUPERSEDES ANY INFORMATION YOU HAVE RECEIVED RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT, EXCEPT IF THIS AGREEMENT IS SUPERSEDED IN ITS ENTIRETY BY ANOTHER WRITTEN AGREEMENT, EXECUTED BY BOTH YOU AND CA, GRANTING YOU A LICENSE TO USE THE PROGRAM. THIS AGREEMENT MAY ONLY BE AMENDED BY A WRITTEN AGREEMENT SIGNED BY AUTHORIZED REPRESENTATIVES OF BOTH PARTIES.

Contents

Preface

Snap Appliance's Snap Servers 4200, 4400, 4500, and 14000 are dedicated storage appliances designed for rapid deployment.

Audience

This guide is intended for system and network administrators charged with installing and maintaining Snap Servers on their network. We assume the administrator is familiar with the basic concepts and tasks of multiplatform network administration.

Purpose

This guide provides information on the installation, configuration, security, and maintenance of Snap Servers. It also provides information on installing and using the following utilities and software components:

- NASManager
- Administration Tool
- Backup Express for GuardianOS
- *e*Trust Inoculate*IT*

Tips and Cautions

This manual uses the following conventions:

Tip A tip presents time-saving shortcuts related to the main topic.

Caution A caution alerts you to potential hardware or software issues or hazards in the configuration or operation of Snap Servers. Consider cautions carefully before proceeding with any operation.

Document Organization

This document is organized as follows:

- **Chapter 1, Getting Started**, provides a brief introduction to Snap Server software features and components, and provides instructions for installing and using Snap Server management utilities.
- **Chapter 2, Setup and Initial Configuration**, shows you how to unpack, install, and then connect to a Snap Server. Information and instructions on completing the Initial Setup Wizard, configuring a UPS device, and registering your server are also provided.
- **Chapter 3, Networking Options**, explains your options for configuring TCP/IP addressing, network bonding, and access protocols for Windows, NFS, Macintosh, FTP, and Web clients.
- **Chapter 4, Storage Configuration and Management**, explains the default storage configuration, how to create a different configuration, and how to maintain the health of RAIDs and manage volume usage.
- **Chapter 5, Security Management**, explains your options for configuring Snap Server security, including local, Windows domain, Windows ADS, and NIS authentication; Web security and encryption (HTTPS); share access definitions; antivirus protection; and support for access control lists.
- **Chapter 6, Data Protection**, explains how to use Snap Server Snapshot technology in conjunction with Backup Express for GuardianOS to back up your data, create the files you need to recover a Snap Server's configuration information, and, if disaster strikes, reinstall the Snap Server operating system and restore the server to its original configuration.
- **Chapter 7, Monitoring and Maintaining Snap Servers**, describes how to configure e-mail notification in response to specific events; review system status, volume usage, and the event log; hot swap hardware components; and reset the system to the factory defaults.
- **Chapter 8, Troubleshooting**, provides solutions to Snap Server installation, set up, networking, security, and maintenance issues.
- **Appendix A, Snap Server Specifications,** lists the Snap Server hardware specifications in detail.
- **Appendix B, Third-Party Backup Applications,** describes how to install the following third party backup agents: CA Brightstor ARCserve, Legato NetWorker, VERITAS NetBackup, and Backup Exec.
- **Appendix C, Upgrading Backup Express for Jukebox Support,** describes how to upgrade Backup Express for GuardianOS to jukebox support.

This document concludes with a glossary and an index.

Typographical Conventions

This manual uses the following conventions.

Font convention	Usage
Bold	Emphasis
Italic	• Emphasis • The introduction of a new terms • Settings you select in the Administration Tool
Arial Bold	Menu commands, command buttons, and navigational links.
Arial	• Text that you type directly into a text field, a command line, or web page • Buttons on a keyboard
`Courier Italic`	A variable for which you must substitute a value
`Courier Bold`	Commands you enter in a command-line interface

Related Documents

Documents related to Snap Server models 4400 and 14000 are shown below.

Title (Part No.)	Description	Format/Location
Snap Server 14000 Quick Start Guide (70990572-001)	Installation and initial configuration instructions for the Snap Server 14000	Printed document / Snap Server carton
Snap Server 4400 Quick Start Guide (70990569-001)	Installation and initial configuration instructions for the Snap Server 4400	Printed document / Snap Server carton
Snap Server 4200/4500 Quick Start Guide (70990625-001)	Installation and initial configuration instructions for Snap Servers 4200 and 4500	Printed document / Snap Server carton
Snap Server Online Help (n/a)	Help for the Administration Tool installed on the Snap Server	HTML document / browser-based Administration Tool
ReadMeFirst.html (70990592-003)	Important information regarding the Snap Server User CD	HTML document / User CD
ReleaseNotes.html (n/a)	Release notes and other important information regarding the latest version of the GuardianOS	HTML document / User CD
Upgrade.html (70990593-003)	Upgrade procedures for the GuardianOS	HTML document / User CD
Install.html (70990593-003)	Installation procedures for NASManager	HTML document / User CD
Backup Express for GuardianOS Getting Started Guide (70990602-001)	Installation and initial configuration instructions for using Backup Express in conjunction with the Snap Server	Printed document / Backup Express CD case
PowerQuest DataKeeper Quick Start Guide (70990605-001)	Installation instructions for using DataKeeper in conjunction with Snap Servers	Printed document / Snap Server carton
Field Replacement Guides (n/a)	Service documents tailored to your Snap Server model. Should the need arise to replace a component, the appropriate document will be included with the part.	Service documents tailored to your Snap Server model

Contacts

Snap Appliance company contacts are listed below.

Snap Appliance Corporate Headquarters

Snap Appliance, Inc.
2001 Logic Drive
San Jose, CA 95124

1.888.310.SNAP (7627) (North America)
408-879-8700 (International)

Snap Appliance Web Site

http://www.snapappliance.com

Service and Technical Support

For an immediate response to a service inquiry, use our Expert Knowledge Base System at http://www.snapappliance.com/support. Simply type in your question to view a list of possible resolutions to known issues. However, if none of the listed topics resolves your inquiry, you can forward the question to our technical support department who will then e-mail you with a response. To obtain additional service or technical support for your Snap Server, call 1.888.338.SNAP (7627) (North America) or 408-558-4657 (International).

Chapter 1

Getting Started

Snap Servers provide a low-cost, low-maintenance network file sharing solution that supports simultaneous access by Windows clients, UNIX/Linux workstations, and Macintosh clients. Snap Servers 4200, 4400, and 4500 provide enterprise security, management, and performance in a 1U form factor; the Snap Server 14000 in a 3U form factor.

Snap Server 14000

Snap Server 4200, 4400, 4500

Snap Servers 4200, 4400, and 4500 support four disks, the 14000 twelve. The 14000 also has an LCD on the front panel that displays its IP address, server name, system status, and error notifications.

Snap Server Features

These models are designed as flexible, network file servers optimized for performance and efficiency. These Snap Servers run the Linux-based GuardianOS, and are designed to maximize file I/O throughput across multi-network protocols. To this end, all unnecessary system control and processing functions that are associated with a general purpose server have been removed. The result is network storage with greater performance, far less maintenance, and higher reliability.

Networking

Snap Servers deliver **multiplatform file sharing** for heterogeneous Windows, UNIX/Linux, and Macintosh environments, enabling fast, seamless deployment into your existing infrastructure. The GuardianOS utilizes **dual-Gigabit Ethernet** technology to support standalone, load balancing, and failover network bonding modes. For more information, see "Networking Options" on page 37.

Storage

Because of **flexible RAID configurations** and hot-swappable disk drives, Snap Servers maintain high data availability.

- RAID 5 (disk striping with parity): For each array, the capacity of one disk is reserved for parity checking
- RAID 1 (disk mirroring): One disk's data replicated to one or more drives
- RAID 0 (disk striping): Large, virtual disk with data striped across all drives of the array; no loss in usable capacity

RAID 1 and 5 configurations can also designate a member disk as a **hot spare** that automatically assumes the role of failed disk. Snap Server servers employ log-based, byte-level journaling file system that is ideal for high-performance, transaction-oriented systems and enables quick file system restarts. For more information, see "Storage Configuration and Management" on page 53.

Security

Snap Servers offers multiplatform authentication options that include local, **Windows domain, Active Directory Service (ADS),** and **Network Information Service (NIS)**, as well as Web security and encryption (HTTPS); flexible share access definitions; native antivirus protection with *e*Trust Inoculate*IT*, and file and folder security. For more information, see "Security Management" on page 73.

Data Protection

Snap Servers enable fast, sure data backup via native **Snapshot** technology, **Backup Express for** GuardianOS, **Server-to-Server Synchronization** software, and third-party network backup agent support. Native **disaster recovery tools** that can ensure complete recovery from a catastrophic event are also provided. For more information, see "Data Protection" on page 93.

Management Applications and Services

Snap Servers offer two separate but integrated interfaces for server configuration. These easy-to-use utilities provide access to all administrative functions. NASManager is java-based utility for discovering and monitoring Snap Servers. The Administration Tool is a browser-based utility for server configuration and ongoing maintenance, such as monitoring server conditions, configuring e-mail alerts for key events or for SNMP management. See the following section for more information on installing and using these utilities. For more information on maintenance screens in the Administration Tool, see "Monitoring and Maintaining Snap Servers" on page 121.

What's New in the GuardianOS 2.4 Release

The major enhancements listed in the following table have been included in the current release of the GuardianOS.

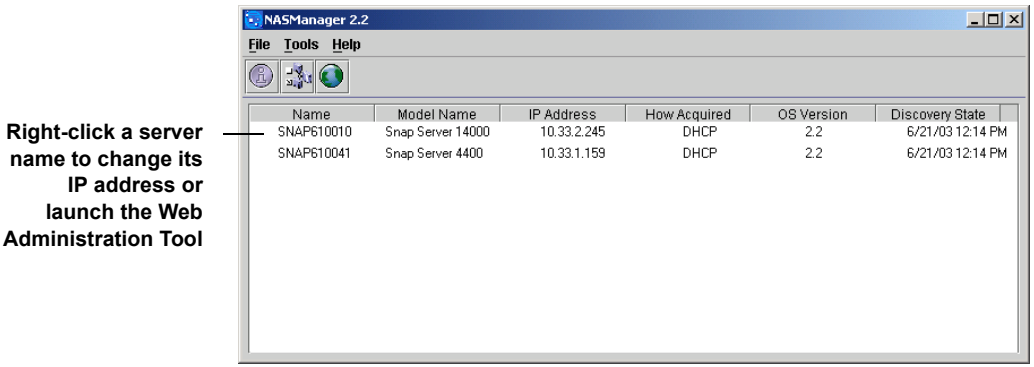
Feature	Description	Page
Mixed Share-Level Access Permissions	Administrators can now assign a mix of read-only and read-write access permissions to users and groups at the share level. (Formerly, only one type of access could be used for share-level security.)	85
Enable Guest Authentication	Allows Windows users to connect to the Snap Server as *guest* (with no password).	81
Domain User Account	Allows administrators using Windows domain authentication to add a user account to ensure that the Snap Server can access domain lists.	81
Reset ACLs to Factory Defaults	Allows administrators to reset file & folder-level security to full control for all users.	126

Installing and Using Snap Server Management Applications

Snap Appliance provides two utilities for discovering, configuring, and troubleshooting Snap Servers. NASManager provides automatic discovery of Snap Servers; the browser-based Administration Tool provides easy access to regular configuration tasks.

NASManager

NASManager is a Java-based, platform-independent application that you use to discover Snap Servers and to perform basic administration tasks, such as setting an IP address or rebooting the server. At startup, NASManager provides a list of all Snap Servers (Guardian OS only) that operate within a given network segment.



Installing NASManager

You can download and install NASManager using the Install.html file found on your Snap Server User CD. NASManager can be installed to all client platforms, including Windows, Macintosh, Linux, and UNIX. The installation program allows you to download the required Java Virtual Machine (JVM) for each platform as necessary.

Launching NASManager

Launch NASManager using one of the methods described in the following table:

Operating System	Procedure
Microsoft Windows XP/Me/ 2000/95/98/NT	Click **Start**. Point to **Programs > NASManager**, then select NASManager.
Macintosh	Open the NASManager folder and double-click the NASManager icon.
UNIX/Linux	For default options: cd to home directory, then run the NASManager command: **`./runNASManager`** If you selected not to create links: cd to home directory, then cd to the NASManager directory, and run the NASManager command: **`./NASManager`**

Using NASManager

Use NASManager to perform the following tasks. Detailed instructions for performing these tasks are provided in the NASManager online help.

- **Discovering Snap Servers —** At startup, NASManager broadcasts discovery request packets to its local network segment; Snap Servers on the same network segment that receive discovery requests respond with information. You can add other Snap Servers (Guardian OS only) that reside outside the local network segment by entering their IP addresses in NASManager's Remote Server List.
- **Getting Information —** This function is a read-only screen that displays information about the server, including the server hardware, GuardianOS version, and server status. It also provides network information, such as IP address, gateway and Ethernet address of the primary Ethernet port.
- **Setting IP Addresses —** This function allows you to set a DHCP-assigned or a static IP address for the first Ethernet interface (Ethernet1) on a Snap Server.
- **Launching the Administration Tool —** This function opens your Web browser to the Administration Tool for the selected server.

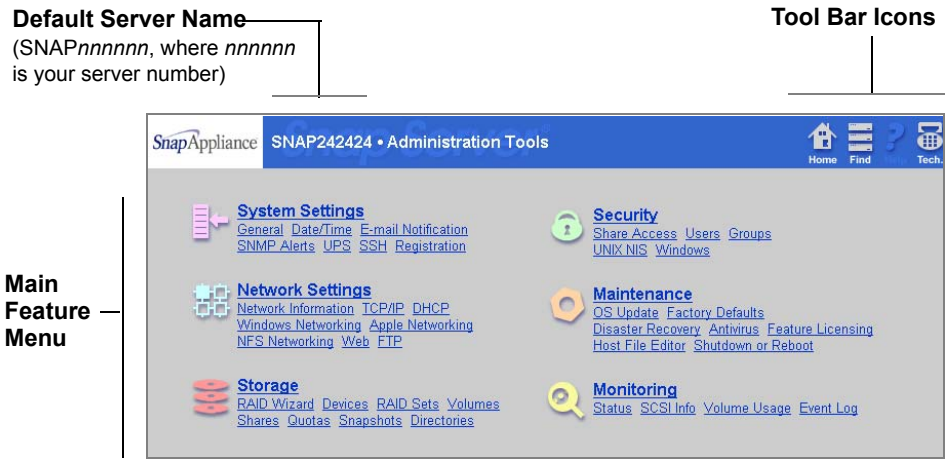
The Administration Tool

The Administration Tool is a browser-based application that allows you to perform a wide range of administrative tasks. The Administration Tool is preinstalled on your Snap Server.

Logging into the Administration Tool

You access the Administration Tool using either of the supported browsers: Microsoft Internet Explorer (4.0 or better), or Netscape Navigator (4.7x or better).

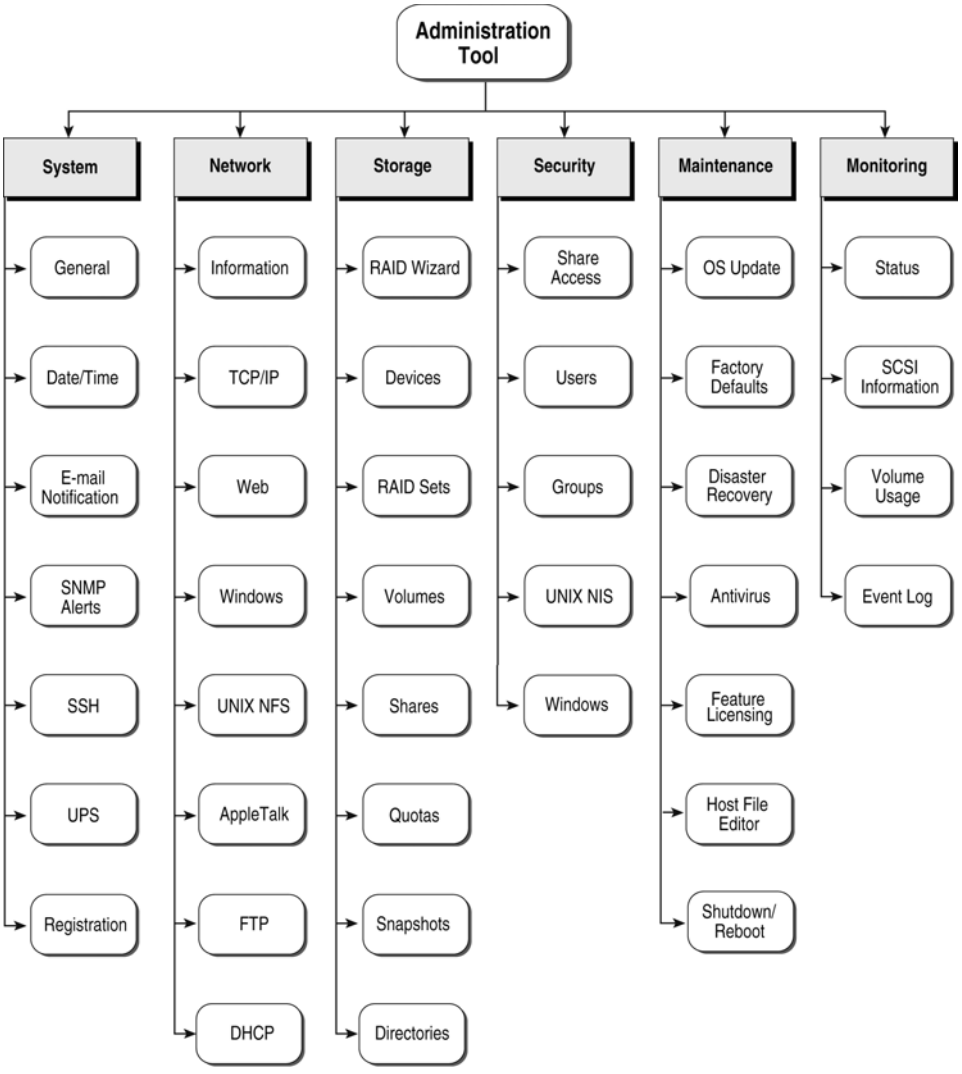
1. Enter a Snap Server name (default is SNAP*nnnnnn*, where *nnnnnn* is your server number) or IP address in your browser. The Web View screen opens. (For information on Web View, see "Web Browser (HTTP)" on page 51.)
2. Click the **Administration** link. The Enter Network Password dialog box opens.
3. Enter the administrator user name and password (default: admin, admin), and click **OK**. The Administration Tool main menu opens.



Tool Bar Icon	
Home	Returns you to the main feature menu (shown above) or the Web View page
Find	Provides access to other GuardianOS Snap Servers
Help	Opens context-sensitive help (Help is not available on navigational screens.)
Tech	Opens to the Snap Appliance technical support Web site

Administration Tool Feature Map

The Administration Tool consists of a set of integrated features that enable you to manage Snap Servers. The following diagram shows the main navigational structure of the Administration Tool interface.

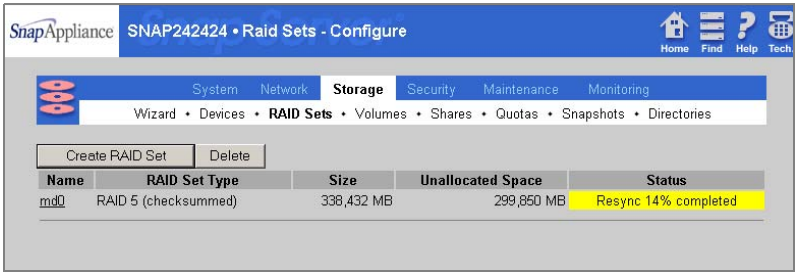


Accessing the Features

You can access Administration Tool features in one of two ways. The following examples show the different navigational paths you can take to access the RAID Sets feature.

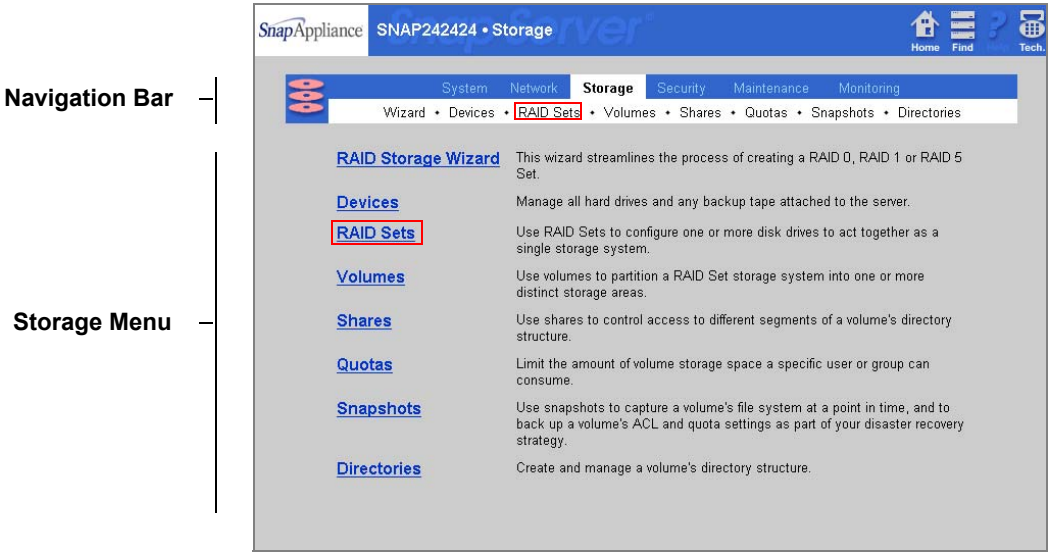
From the Administration Tool main menu

1. After logging into the Administration Tool, the main menu opens. (If you are already logged in, click the Home icon to return to the Administration Tool main menu.)
2. Click the **RAID Sets** link. You are taken directly to the **Storage > RAID Sets** screen.



From the Administration Tool Navigation Bar

1. If necessary, click the **Storage** link in the navigation bar. The Storage menu opens.



2. Click the **RAID Sets** link, either in the Navigation bar or in the menu.

Chapter 2

Setup and Initial Configuration

Snap Servers are designed to be set up, installed, and operational on your network in less than 15 minutes. This chapter covers how to unpack, install, and then connect to a Snap Server. Information and procedures for initial configuration tasks, such as completing the Initial Setup Wizard, configuring a UPS device, and registering your server are also provided.

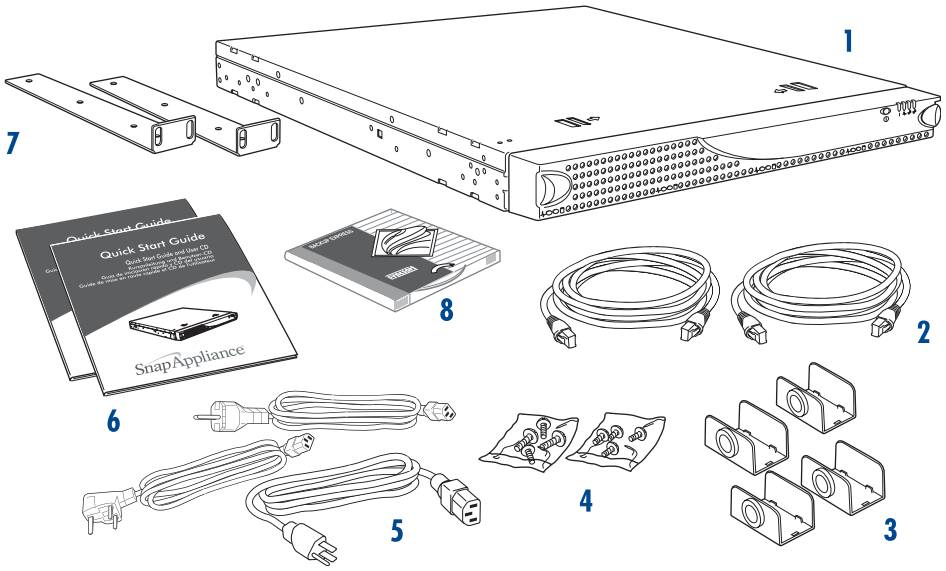
- **Setting Up the Snap Server 4400 —** Provides information about how to unpack, install, and connect to the Snap Server 4400.
- **Setting Up the Snap Server 4200/4500 —** Provides information about how to unpack, install, and connect to the Snap Server 4200/4500.
- **Setting Up the Snap Server 14000 —** Provides information about how to unpack, install, and connect to the Snap Server 14000.
- **Initial Configuration Tasks —** Describes how to use the Initial Setup Wizard to perform essential configuration tasks, such as naming the server, setting the administrator password, entering TCP/IP settings and how to use the Administration Tool to configure your APC-brand uninterruptible power supply (UPS) device.

Tip Snap Servers are designed to work with a network-based, APC-brand UPS. Visit the APC Web site for a listing of optimal APC models for use with your Snap Server.

Setting Up the Snap Server 4400

Snap Server 4400 Hardware Components

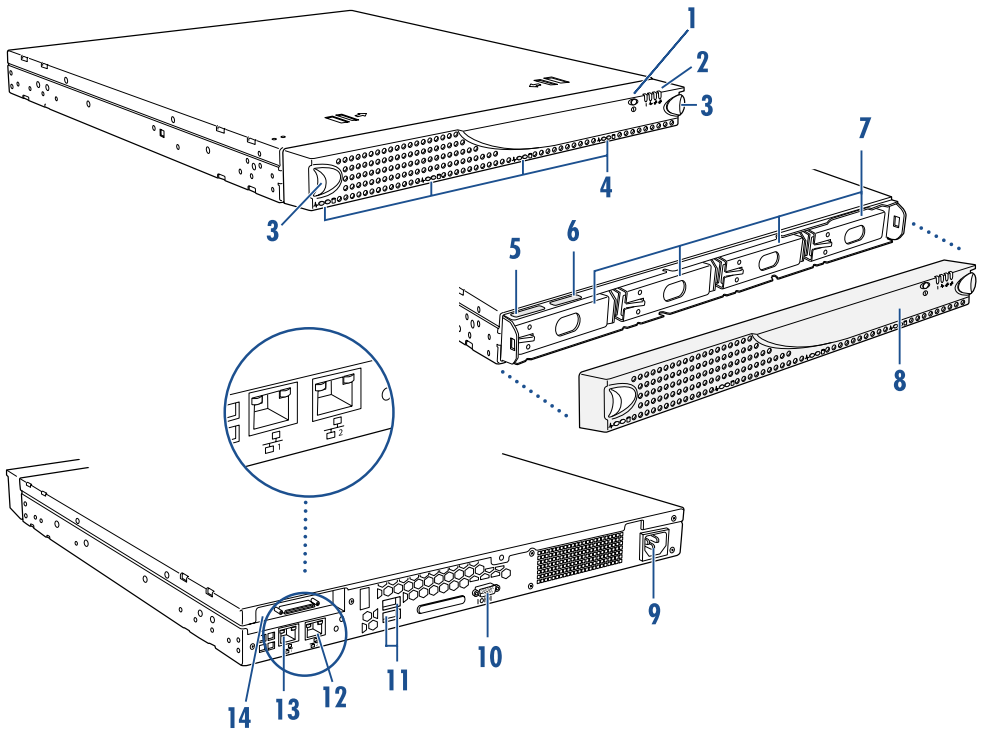
You should have all the items shown in the following illustration:



1. Snap Server 4400
2. Two Ethernet cables
3. Stacking clips
4. Rack mount screws (eight in all: four for mount brackets, four for rack post)
5. Power cords
6. Quick Start Guide, User CD, registration and safety information, and DataKeeper Quick Start Guide and CD
7. Rack mount brackets (left and right)
8. Backup Express CDs

Snap Server 4400 Hardware Features

The following illustration identifies Snap Server 4400 hardware features. Subsequent sections discuss the status lights, and how to connect the server to the network.



1	Power button	8	Front bezel
2	System LEDs (status lights)	9	Power connector
3	Release latches	10	Service connector
4	Disk drive status lights	11	USB connectors (disabled)
5	Server number label[a]	12	Ethernet2 connector
6	Serial number label[b]	13	Ethernet1 connector (primary)
7	Hot-swappable disk drives (four)	14	SCSI connector (optional on some models)

a. To access this label, remove the front bezel. The server number is comprised exclusively of numerics.

b. To access this label, remove the front bezel. The 10-character alphanumeric serial number appears on the second label.

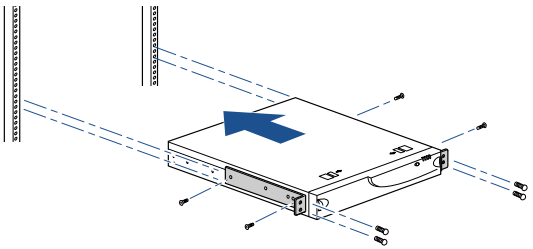
Rack Installation for the Snap Server 4400

The Snap Server 4400 ships with two L-shaped rack mount brackets. You can attach them in one of two ways: (1) to the front of the server for mounting to the front posts of a four-post rack; or, (2) to the middle or front of the server for mounting to both posts of a Telco rack.

Caution The following procedure applies to standard EIA racks; other racks may not be able to support the server using only the front posts. If you are using a non-EIA rack, Snap Appliance recommends that you secure the server using slide rails, available from Snap Appliance or a Snap Appliance reseller.

1 Make sure you have the following items necessary for rack installation:

- Two (left and right) front rack mounting bracket assemblies
- Four rack ear screws to attach the brackets to the server
- Four rack mounting screws to attach the brackets to the rack posts
- One Phillips screwdriver



2 Attach the L-shaped brackets to the front or to the middle of the server using the four screws provided.

3 Insert the server into the rack and attach the server to the posts using the remaining four screws. You may need a second person to support the server while tightening down the mounting screws.

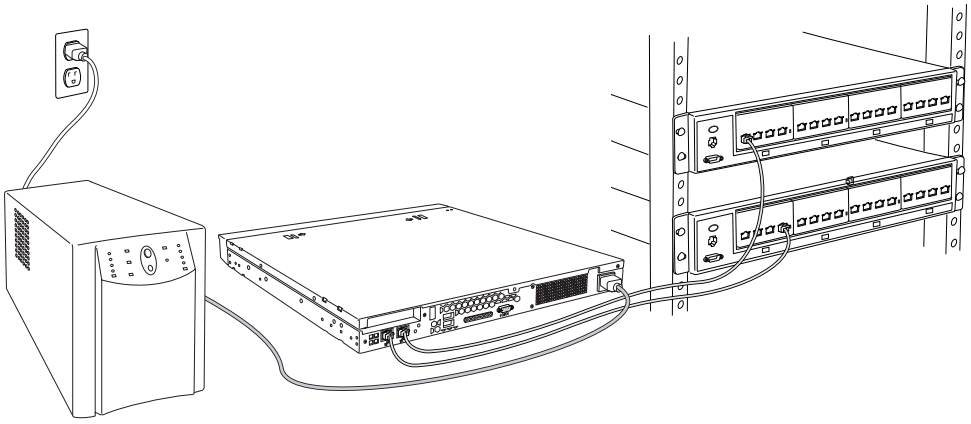
Connecting to the Network

The server has dual-Ethernet ports that can connect to 10BaseT, 100BaseTx, or 1000BaseT networks. A dual-port configuration offers added advantages, such as load balancing and failover. You may connect one or both of the ports.

- If you connect only one port, you must use the primary port (see page 11 for location).
- If you connect both ports and plan to use a bonded configuration, make sure that both ports are physically connected to the network on the same subnet. For additional information, see "Understanding Dual-Ethernet Bonding Options" on page 39.

Caution The speed/duplex setting on Snap Servers defaults to *autonegotiate*. The networking switch or hub to which the server is connected must also be configured to autonegotiate; otherwise, network throughput or connectivity to the server may be seriously impacted.

Use the provided Ethernet cables to connect the server to the network. When you connect the network cables to active ports, the network lights on the bezel (LAN 1 and LAN 2) are green.



Connecting to the Power Supply

As a data security measure, Snap Appliance strongly recommends you connect the Snap Server to the power source via a UPS. (If no UPS is available, connect the power cord to a properly grounded electrical outlet.)

Tip Snap Servers are optimized to work with APC-brand, network-based UPS devices. If you choose this option, you must configure the APC unit in the Snap Server's Administration Tool *and* in the APC user interface. For details, see "Configuring your APC-Brand UPS Device" on page 34.

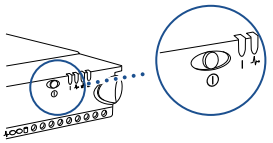
To Connect the Power Supply to a UPS

1. Plug the power cord (female end) into the power connector on the server.
2. Plug the power cord (male end) into a UPS or a properly grounded electrical outlet.

Initializing the Snap Server 4400

Use the power button on the front of the server to power on and power off the server.

To turn on the server, press the power button on the front of the server. The server takes a few minutes to initialize.



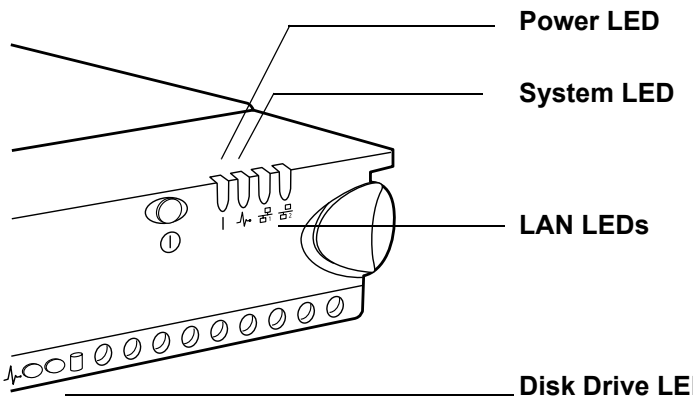
- A green power LED indicates that the system is on.
- An amber system LED indicates a system error.

To turn off the server, press and release the power button to begin the shutdown process. Do not depress this button for more than four seconds.

Tip The Snap Server 4400 has a persistent power state. When a physical loss of power occurs, the Snap Server returns to the same operation it had when the power went out. Therefore, if the system is powered down prior to a power loss, it will remain powered down when the power is restored.

Understanding the Snap Server 4400 Status and Drive Lights

The server has two status lights, two network lights, and two lights for each of the four disk drives, as shown in the following illustration:



Snap Appliance recommends that you become familiar with the operation of these lights.

Power, System, and LAN LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED. They operate as follows:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Blinking green (once per second)	The server is booted up and operating normally.
Solid amber	The server has encountered a system error.
Blinking amber	The server has booted to Maintenance mode. For more information, see “Disaster Recovery Procedures” on page 116.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network.
Flashing green	There is activity between the system and other devices on the network.
Off	The port is disconnected or the Ethernet cable is not connected/ linked to an active hub or switch.

Disk Drive LEDs

The Snap Server 4400 has two lights below each disk drive. The left light indicates power. The right light indicates drive activity. They operate as follows:

Power LED (left)	**Activity LED (right)**	
Solid green	Off	Disk drive installed properly but is not active
Solid green	Flashing amber	Disk drive installed properly and actively reading/writing information
Solid amber	Off	Disk drive installed, but not working properly
Off	Off	No disk drive installed

Connecting to the Snap Server 4400

To connect to a Snap Server 4400, you need either the server's name or IP address. The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number. For example, the name of a Snap Server with a server number of 610019 is SNAP610019. The server's IP address can be discovered using NASManager.

1 **Do one of the following:**

To use the server name:

Tip This procedure requires that name resolution services via WINS or a name broadcast be operational.

a Locate the serial number by removing the bezel on the front of the server.

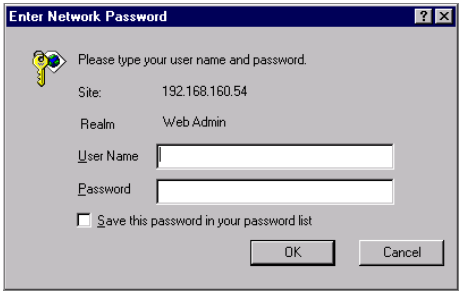
b Append the first six digits of the number to the string: SNAP.

c In a Web browser, enter the name and click Enter.

To use the IP address:

a Discover the server's IP address by installing (on the same subnet as the Snap Server) and launching NASManager, as described on page 4.

b In the NASManager console, right-click the server name and select **Administer via Web Browser**. The Enter Network Password dialog box opens.



2 **Log into the Administration Tool.**

Enter admin as the user name and admin as the password.

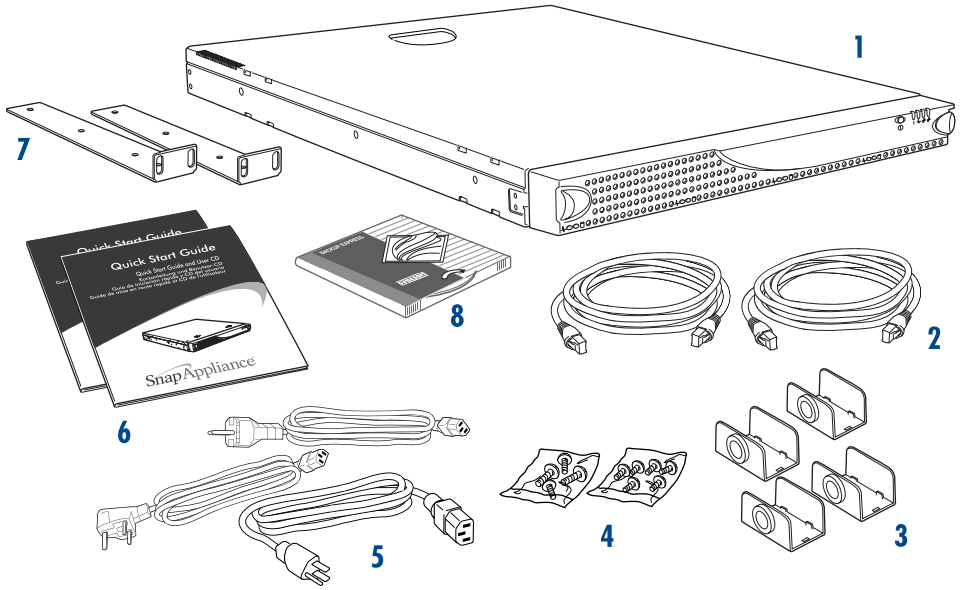
3 **Complete the initial configuration procedures.**

Instructions for using the Initial Setup Wizard are found on page 30.

Setting Up the Snap Server 4200/4500

Snap Server 4200/4500 Hardware Components

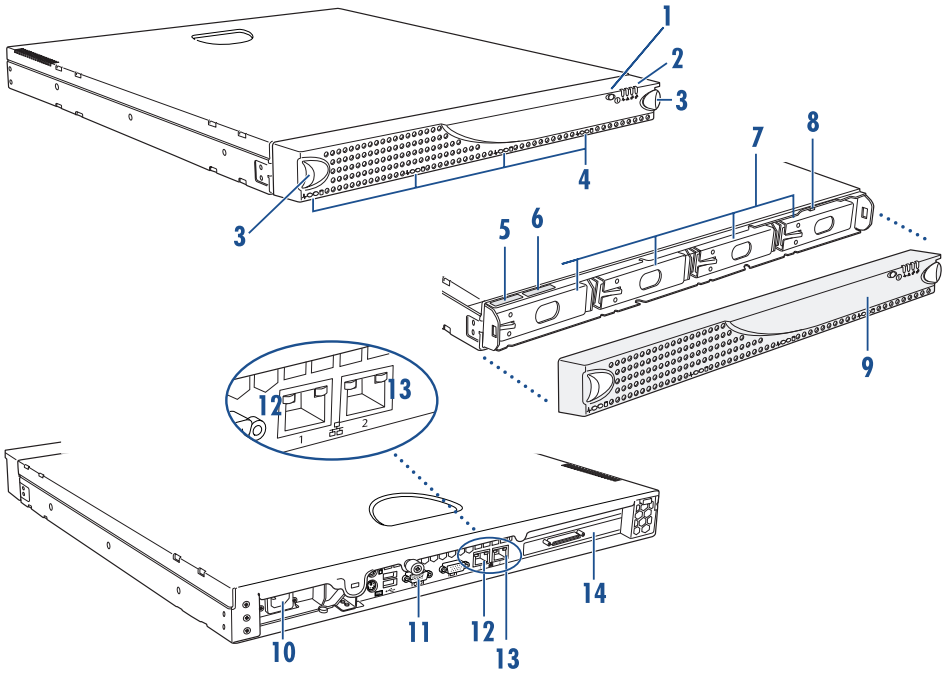
You should have all the items shown in the following illustration:



1. Snap Server 4200/4500
2. Two Ethernet cables
3. Stacking clips
4. Rack mount screws (ten in all: six for mount brackets, four for rack post)
5. Power cords
6. Quick Start Guide, User CD, registration and safety information, and DataKeeper Quick Start Guide and CD
7. Rack mount brackets (left and right)
8. Backup Express CDs

Snap Server 4200/4500 Hardware Features

The following illustration identifies Snap Server 4200/4500 hardware features. Subsequent sections discuss the status lights, and how to connect the server to the network.



1	Power button	8	Reset Button (White)
2	System LEDs (status lights)	9	Front Bezel
3	Release latches (two)	10	Power connector
4	Disk drive status lights	11	Service connector
5	Server number label[a]	12	Primary Ethernet connector
6	Serial number label[b]	13	Secondary Ethernet connector
7	Hot-swappable disk drives (four)	14	SCSI connector (optional on some models)

a. To access this label, remove the front bezel. The server number is comprised exclusively of numerics.

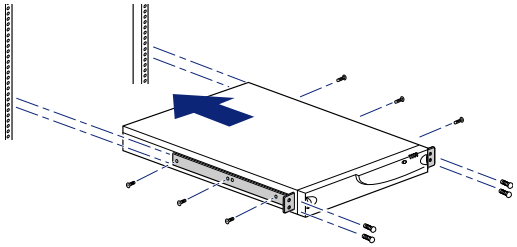
b. To access this label, remove the front bezel. The 10-character alphanumeric serial number appears on the second label.

Rack Installation for the Snap Server 4200/4500

The Snap Server 4200/4500 ships with two L-shaped rack mount brackets. You can attach them in one of two ways: (1) to the front of the server for mounting to the front posts of a four-post rack; or, (2) to the middle or front of the server for mounting to both posts of a Telco rack.

Caution The following procedure applies to standard EIA racks; other racks may not be able to support the server using only the front posts. If you are using a non-EIA rack, Snap Appliance recommends that you secure the server using slide rails, available from Snap Appliance or a Snap Appliance reseller.

1. Make sure you have the following items necessary for rack installation:
   - Two (left and right) front rack mounting bracket assemblies
   - Six rack ear screws to attach the brackets to the server
   - Four rack mounting screws to attach the brackets to the rack posts
   - One Phillips screwdriver



2. If mounting the L-shaped brackets to the front of the server (as shown in the illustration), use the six screws provided. (If mounting to the middle of the server (not shown) for installation into a Telco rack, only four screws are used.)
3. Insert the server into the rack and attach the server to the posts using the remaining four screws. You may need a second person to support the server while tightening down the mounting screws.

Connecting to the Network

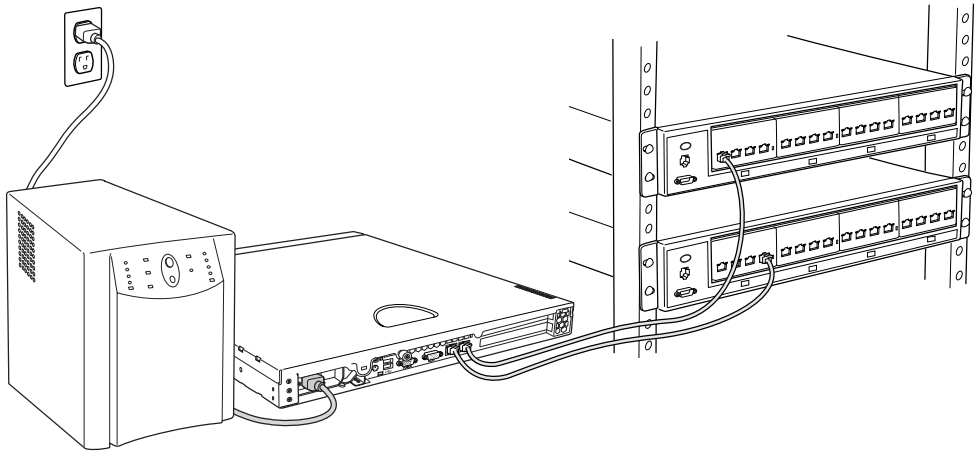
The server has dual-Ethernet ports that can connect to 10BaseT, 100BaseTx, or 1000BaseT networks. A dual-port configuration offers added advantages, such as load balancing and failover. You may connect one or both of the ports.

- If you connect only one port, you must use the primary port (see page 11 for location).

- If you connect both ports and plan to use a bonded configuration, make sure that both ports are physically connected to the network on the same subnet. For additional information, see "Understanding Dual-Ethernet Bonding Options" on page 39.

Caution The speed/duplex setting on Snap Servers defaults to *autonegotiate*. The networking switch or hub to which the server is connected must also be configured to autonegotiate; otherwise, network throughput or connectivity to the server may be seriously impacted.

Use the provided Ethernet cables to connect the server to the network. When you connect the network cables to active ports, the network lights on the bezel (LAN 1 and LAN 2) are green.



Connecting to the Power Supply

As a data security measure, Snap Appliance strongly recommends you connect the Snap Server to the power source via a UPS. (If no UPS is available, connect the power cord to a properly grounded electrical outlet.)

Tip Snap Servers are optimized to work with APC-brand, network-based UPS devices. If you choose this option, you must configure the APC unit in the Snap Server's Administration Tool *and* in the APC user interface. For details, see "Configuring your APC-Brand UPS Device" on page 34.

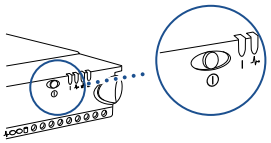
To Connect to the Power Supply Via a UPS

1. Plug the power cord (female end) into the power connector on the server.
2. Plug the power cord (male end) into a UPS or a properly grounded electrical outlet.

Initializing the Snap Server 4200/4500

Use the power button on the front of the server to power on and power off the server.

To turn on the server, press the power button on the front of the server. The server takes a few minutes to initialize.



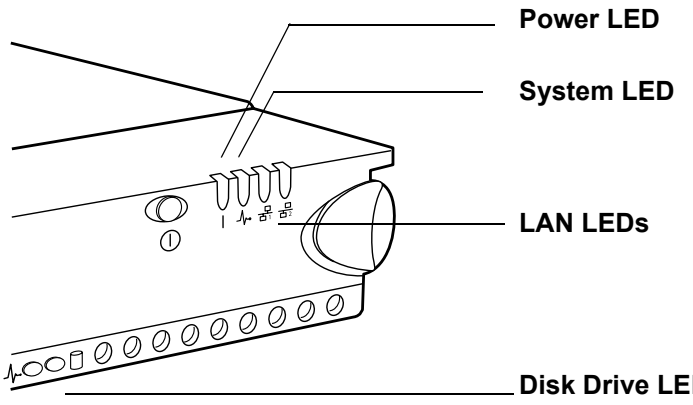
- A green power LED indicates that the system is on.
- An amber system LED indicates a system error.

To turn off the server, press and release the power button to begin the shutdown process. Do not depress this button for more than four seconds.

Tip The Snap Server 4200/4500 has a persistent power state. When a physical loss of power occurs, the Snap Server returns to the same operation it had when the power went out. Therefore, if the system is powered down prior to a power loss, it will remain powered down when the power is restored.

Understanding the Snap Server 4200/4500 Status and Drive Lights

The server has two status lights, two network lights, and two lights for each of the four disk drives, as shown in the following illustration:



Snap Appliance recommends that you become familiar with the operation of these lights.

Power, System, and LAN LEDs

These status lights are located to the right of the power button. Looking at the server from the front, the lights appear in the following order, from left to right: power LED, system LED, LAN 1 (Ethernet1) LED, and LAN 2 (Ethernet2) LED. They operate as follows:

Power LED	
Solid green	The server is powered on.
Off	The server is powered off.

System LED	
Blinking green (once per second)	The server is booted up and operating normally.
Solid amber	The server has encountered a system error.

LAN 1 and LAN 2 LEDs	
Solid green	The server is active and connected to the network on the LAN 1 port.
Off	The port is disconnected or the Ethernet cable is not connected/ linked to an active hub or switch.

Disk Drive LEDs

The Snap Server 4200/4500 has two lights below each disk drive. The left light indicates power. The right light indicates drive activity. They operate as follows:

Power LED (left)	**Activity LED (right)**	
Solid green	Off	Disk drive installed properly but is not active
Solid green	Flashing amber	Disk drive installed properly and actively reading/writing information
Solid amber	Off	Disk drive installed, but not working correctly
Off	Off	No disk drive installed

Connecting to the Snap Server 4200/4500

To connect to a Snap Server 4200/4500, you need the server's name or IP address. The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number. For example, the name of a Snap Server with a server number of 610019 is SNAP610019. The server's IP address can be discovered using NASManager.

1 **Do one of the following:**

To use the server name:

Tip This procedure requires that name resolution services via WINS or a name broadcast be operational.

a Locate the serial number by removing the bezel on the front of the server.

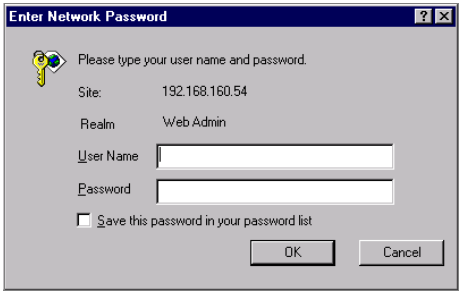
b Append the first six digits of the number to the string: SNAP.

c In a Web browser, enter the name and click Enter.

To use the IP address:

a Discover the server's IP address by installing and launching NASManager, as described on page 4.

b In the NASManager console, right-click the server name and select **Administer via Web Browser**. The Enter Network Password dialog box opens.



2 **Log into the Administration Tool.**

Enter admin as the user name and admin as the password.

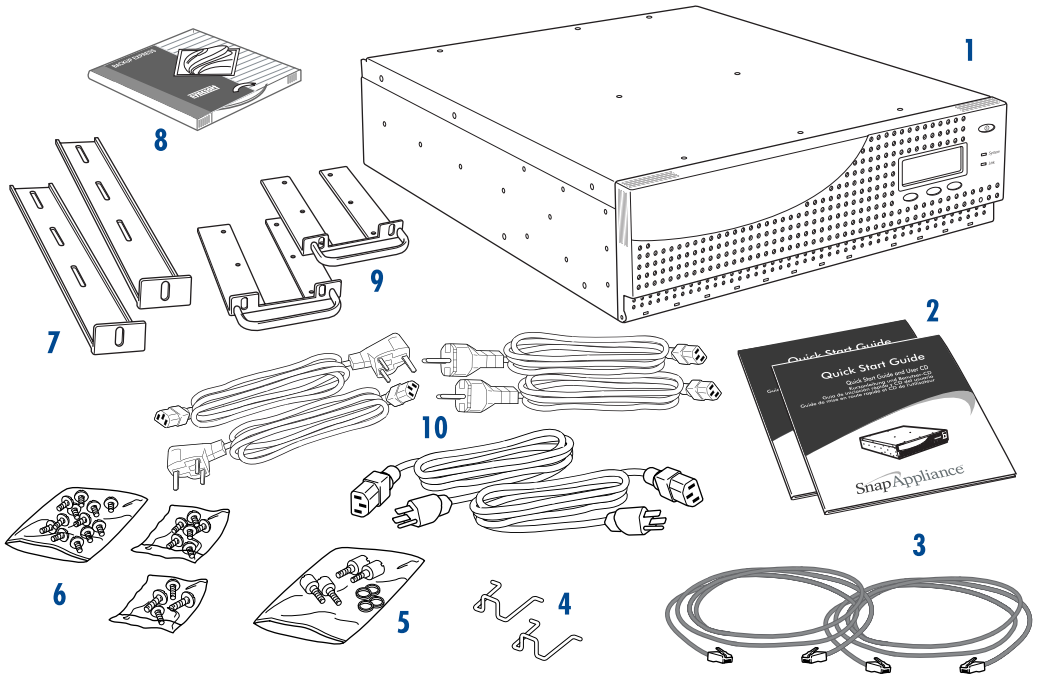
3 **Complete the initial configuration procedures.**

Instructions for using the Initial Setup Wizard are found on page 30.

Setting Up the Snap Server 14000

Snap Server 14000 Hardware Components

You should have all the items shown in the following illustration:



1 Snap Server 14000

2 Quick Start Guide, User CD, registration and safety information, and DataKeeper Quick Start Guide and CD

3 Two Ethernet cables

4 Two power cord clips

5 Four quick-release screw assemblies consisting of the knurled head, the threaded stud, and plastic washer

6 Sixteen black and four rear support mount screws

7 Two long rear support brackets (recommended for use with four-post racks)

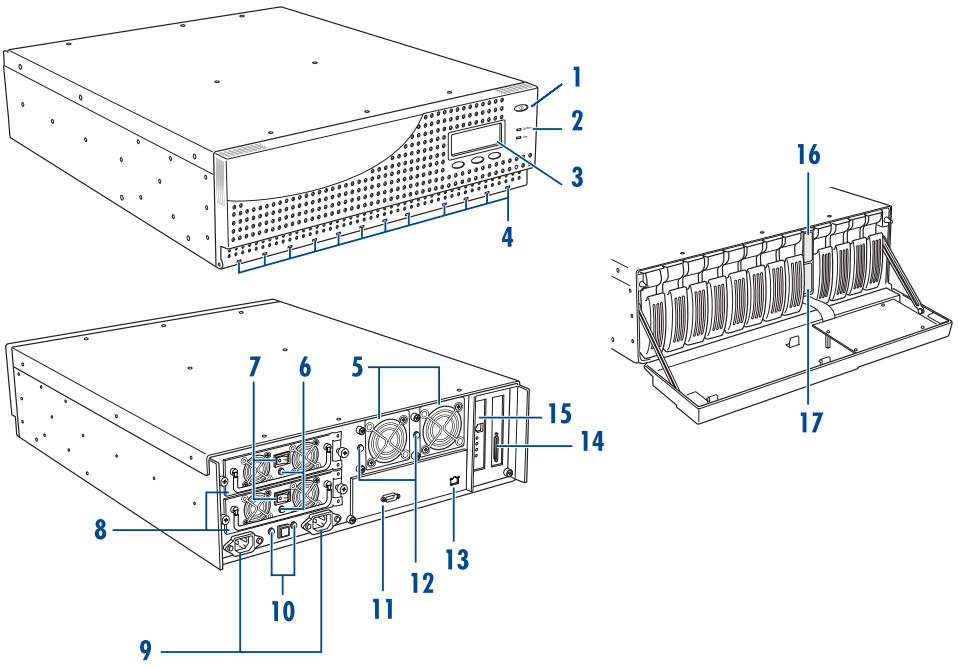
8 Backup Express CDs

9 Two (left and right) front rack mounting bracket/handle assemblies

10 Power cords

Snap Server 14000 Hardware Features

The following illustration identifies Snap Server hardware features.



1 Power button
2 System LEDs (status lights)
3 LCD
4 Disk drive status lights
5 Hot-swappable fans
6 Power supply status lights
7 Power supply on/off switches
8 Power supplies
9 Power connectors
10 Power supply activity lights
11 Service connector
12 Fan status lights
13 Primary Ethernet connector
14 SCSI connector
15 Secondary Ethernet connector
16 Server number label[a]
17 Serial number label[b]

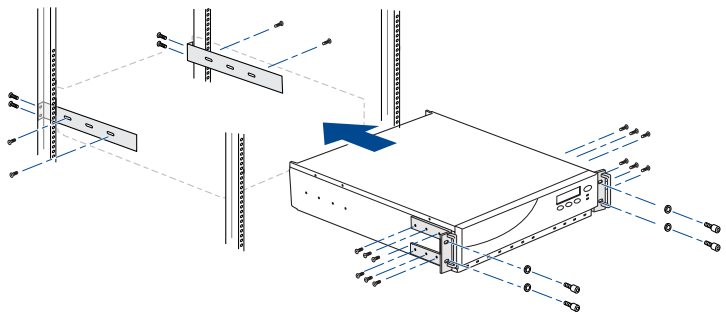
a. To get the server number, open the front door. The server number is comprised exclusively of numerics.
b. To access this label, open the front bezel. The 10-character alphanumeric serial number appears on the second label.

Rack Installation for the Snap Server 14000

Be sure to install the server correctly. The server weighs approximately 75 pounds, and rack installation requires two or more people. If you have a four-post rack, Snap Appliance recommends that you use the rear support brackets provided.

Caution The following procedure applies to standard EIA racks; other racks may not be able to support the server using only the front post. If you are using a non-EIA rack, Snap Appliance recommends that you secure the server using slide rails, available from Snap Appliance or a Snap Appliance reseller.

1. Before installing the rack, make sure you have the following items:
   - Two (left and right) front rack mounting bracket assemblies (ears)
   - Four quick-release screw assemblies (knurled head, threaded stud, and plastic washer)
   - Sixteen black screws (twelve to attach the front rack mounting bracket assemblies and four to attach the long rear support brackets to the sides of the server)
   - Two long rear support brackets, recommended for use with four-post racks
   - One Phillips screwdriver
2. Separate the four quick-release screws into component parts (knurled heads, threaded studs, and plastic washers).



3. Determine the mounting height for the server in the rack, and then mount the threaded studs from the four quick-release screws into the rack at that height.
4. Attach the front bracket assemblies to the front of the server using twelve of the black screws provided (six for each front bracket assembly).
5. With at least one other person, temporarily support the server, and align the slots on the front brackets with the threaded studs of the quick-release screws.

6 Immediately place the plastic washers over the studs and fasten the knurled heads to secure the server to the rack.

If you have a four-post rack, attach the rear support brackets to the rack and then to the server as follows:

7 Align the slots on the rear support brackets with the mounting holes on the server, and then mark the corresponding rear rack post mounting locations.

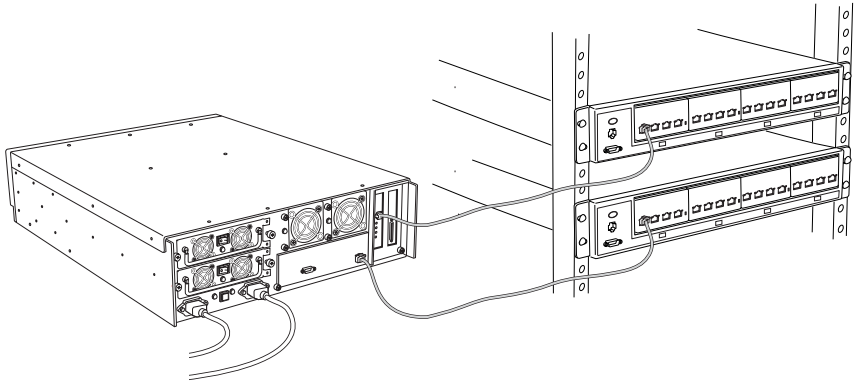
8 Use the four long silver screws to attach the rear support brackets to the back posts of the rack.

9 Use the remaining four black screws to attach the long rear support brackets to the server.

Connecting to the Network

The server has dual-Ethernet ports to connect to 10BaseT, 100BaseTx, or 1000BaseT networks. A dual-port configuration offers important advantages, such as load balancing and failover. You may connect one or both of the ports.

Use the provided Ethernet cables to connect the server to the network, as shown in the following illustration:



- If you connect only one port, you must use the primary port, which is located beneath the two fans (see page 25). If you use Ethernet2, the server's IP address will not appear on the LCD.
- If you connect both ports and plan to use a bonded configuration, make sure that both ports are physically connected to the network on the same subnet. For additional information, see "Understanding Dual-Ethernet Bonding Options" on page 39.

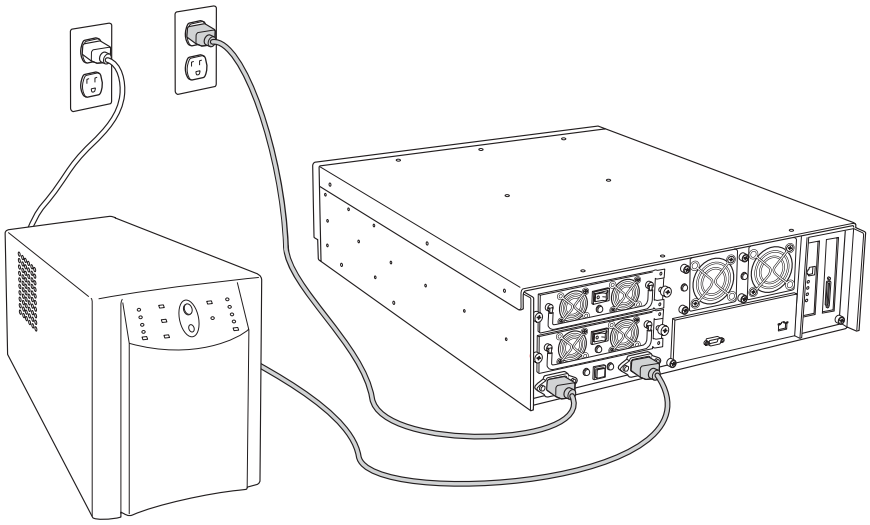
Caution The speed/duplex setting on Snap Servers defaults to *autonegotiate*. The networking switch or hub to which the server is connected must also be configured to autonegotiate; otherwise, network throughput or connectivity to the server may be seriously impacted.

Connecting to the Power Supply

When you connect the Snap Server to a power source, plug the power cords into two different sources. This strategy protects the server if one power source fails.

For the best protection from power failures, connect each power cord to two different UPS devices. Each UPS should have a minimum rating of 160 watt hours. If you have only one UPS, connect one cord to the UPS and the other to a properly grounded electrical outlet. If the UPS option is not available, connect the power cords to two properly grounded electrical outlets on different circuits.

1 Plug the power cords (female ends) into the power connectors on the server.



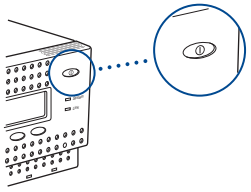
2 Plug the power cords (male ends) into properly grounded electrical outlets.

Tip Do not plug both cords into the same multiple-outlet surge protector or one two-socket wall outlet. To do so negates the benefits of dual power supplies.

Initializing the Snap Server 14000

To initialize the Snap Server 14000, use the following procedure:

1. Make sure the power switches on both power supplies are in the **on** position (the 1 on the toggle switch is depressed).
2. Depress the front power button until the LCD illuminates (about three seconds).
3. Wait for the server to initialize (a few minutes).



Using the Snap Server 14000 LCD

The LCD provides status information and event logs. When the Snap Server 14000 is turned on, the LCD displays the server name, IP address, and the workgroup or domain.

Observe the three buttons below the LCD. To view details on any event, press the center button. Use the right button to scroll down the events. Press the left button to return to the status information.

Connecting to the Snap Server 14000

Connecting to the Snap Server 14000 involves obtaining the server's IP address from the LCD and connecting to the server via the Administration Tool.

1. Get the Snap Server's IP address from the LCD.

   The LCD panel on the front of the Snap Server 14000 displays its IP address.

   Tip If the LCD shows the default IP address of 10.10.10.10, it means that no DHCP server was found on the network, and that the Snap Server has not been assigned an IP address. You may not be able to see the server on your network, and thus, you may not be able to access the Administration Tool. In this situation, you must use NASManager as described on page 4 to find the server and assign it a static IP address.

2. Connect to the server using a Web browser:

   In a Web browser, enter the server's IP address using the format: http://1.2.3.4, and press Enter. The Enter Network Password dialog box opens.

3. Log into the Administration Tool.

   Enter admin as the user name and admin as the password, and then click **OK**.

4. Complete the initial configuration procedures.

   Instructions for using the Initial Setup Wizard are found on page 30.

Initial Configuration Tasks

The first time you connect to your Snap Server, the Initial Setup Wizard runs. This wizard presents a series of screens that allows you to quickly establish connectivity and basic security for the server. Once you complete the wizard and reboot the server, Snap Appliance recommends that you immediately configure your UPS device and register your server.

Before You Begin

The Initial Setup Wizard consists of several screens that allow you to change the server name, set the date and time, set the administrator password, and configure TCP/IP settings for the primary Ethernet port (Ethernet1).

Server Name

The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number. For example, the name of a Snap Server with a server number of 610019 is SNAP610019. The server number is located on the server label. To locate the server number, remove the front bezel (4200, 4400, and 4500) or open the front door (14000).

Administrator Password

The default Administrator user name is admin and the default password is also admin. Snap Appliance strongly recommends that you set a new administrator password for your server.

TCP/IP Settings

Snap Servers are preset to use DHCP. If you do not plan to use or do not have a DHCP server, you should assemble the following information prior to running the wizard:

- The IP address for the Snap Server
- The subnet mask
- The default gateway IP address
- The domain server IP address
- WINS server(s) IP address(es)

APC-Brand UPS Configuration

Snap Appliance recommends that you use a UPS with the Snap Server. A UPS is the best way to protect your data from unforeseen power outages. Snap Servers are compatible with network-based, APC-brand uninterruptible power supplies that allow you to take advantage of the automatic shutdown capability. Visit the APC Web site for a listing of optimal APC models for use with your Snap Server. For instructions on configuring you APC-brand UPS device, see page 34.

Server Registration

You must register your server to activate you warranty, receive Snap Care service and support, the resources to create and track service requests, to receive software updates, to receive exclusive promotional offers, and to receive other special services. To register your server, have the following information available:

- **Server number —** A numerics-only string
- **Serial number —** A 10-character alphanumeric string

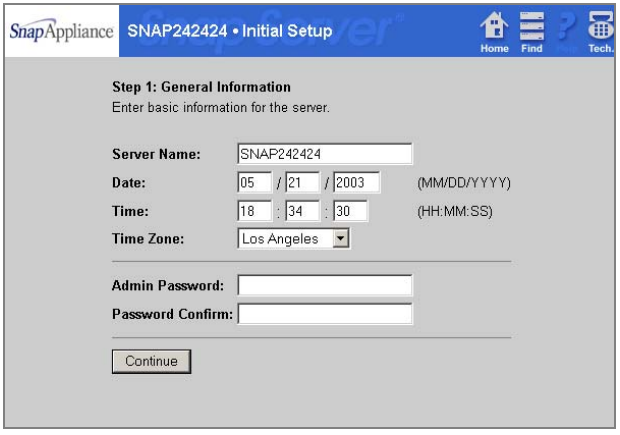
These numbers appear on labels affixed to the inside of your Snap Server. To view the labels, remove the front bezel (4200, 4400, and 4500) or open the front door (14000).

You can register your server as part of the Setup wizard, or at a later time using the **System > Register** screen in the Administration Tool.

Using the Initial Setup Wizard

To complete the Setup wizard, use the following 4-step procedure:

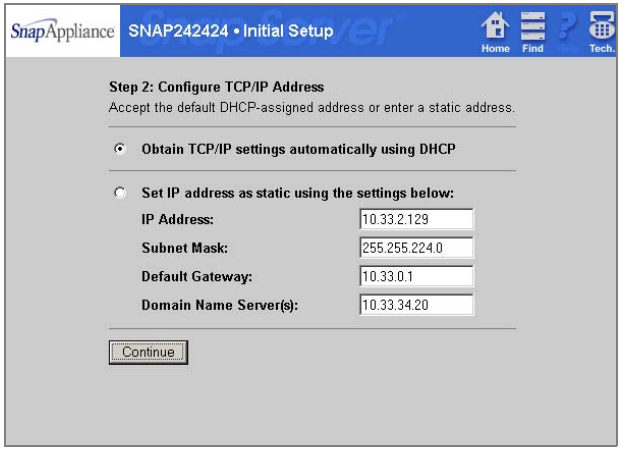
1 **In step 1, enter general server settings.**



- **Server name** — The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number.
- **Time settings** — The time and date default to the settings on the local network. The time zone defaults to Greenwich time.
- **Administrator account and password**—The default Administrator user name is admin and the default password is also admin. Snap Appliance strongly recommends that you set a new administrator password at this time.

Click **Continue** to view the TCP/IP screen.

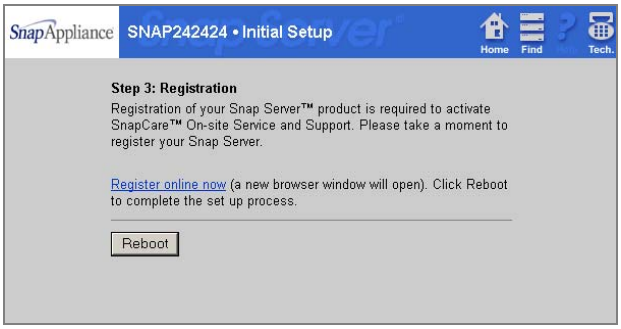
2 **In step 2, configure TCP/IP addressing.**



The default setting is to obtain the TCP/IP settings from the DHCP server. Do one of the following:

- To accept the default DHCP-assigned address, click **Continue** to view the license agreement.
- To enter a static address, select **Set IP address as static using the settings below**. Enter the appropriate information for a static address, as described on page 30. When finished, click **Continue**.

3 **In step 4, register the server.**



Click the **Register online now** link to open a separate browser window that provides instructions on how to proceed. (If you prefer to register the server at a later time, you can do so from the **System > Registration** screen in the Administration Tool.)

4 **Reboot the server.**

Click **Reboot**. The server reboots to the Web View screen.

From this screen, you can log into the Administration Tool and complete initial configuration as described in subsequent sections.

Logging into the Administration Tool

To log into the Administration Tool, use the following procedure:

1 On the Web View screen, click the **Administration** link.

The Enter Network Password dialog box opens.

2 Enter the user name admin and the new password you created using the Initial Setup Wizard.

3 Click **OK**.

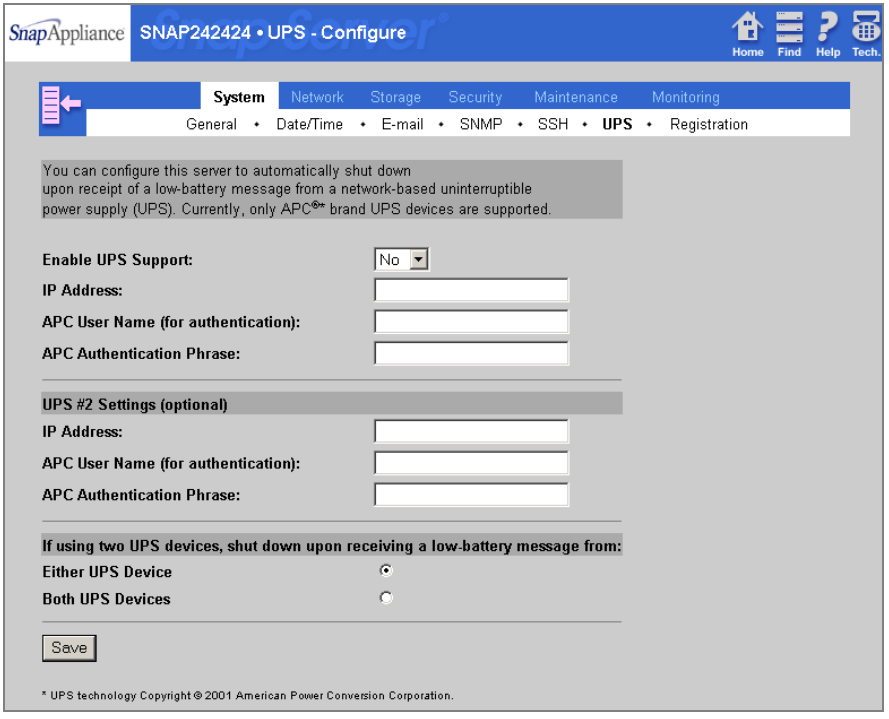
The Administration Tool main menu opens.

Configuring your APC-Brand UPS Device

To configure an APC-Brand UPS device, you must: (1) enable UPS support on the Snap Server as described in this section; and, (2) identify the Snap Server to the APC software. In the APC UPS browser-based user interface, navigate to the Power Chute configuration page, and add the Snap Server's IP address to the client list. If you are using DHCP, entering any IP address on your network will work.

Tip The following procedure describes enabling two UPS devices on the Snap Server 14000. Only steps 1 through 3 apply to Snap Servers 4200, 4400, and 4500 because they have a single power supply.

1 From the Administration Tool main menu, navigate to the **System > UPS** screen.



2 Select *Yes* from the pull-down menu to enable UPS support.

3 Enter the following values for each UPS device:

- IP address
- APC user name
- APC authentication phrase

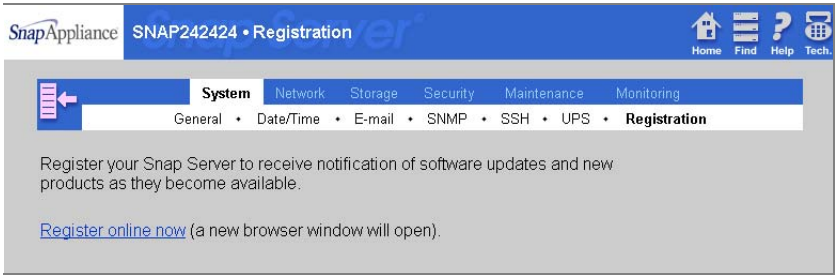
4 If you are using two UPS devices, you can select automatic shutdown upon receiving a message from one or both UPS devices.

5 Click **Save**.

Tip The Snap Server 14000's maximum load is 300 watts. The maximum load for Snap Servers 4200, 4400, and 4500 is 160 watts. To determine how many hours of service your UPS will supply, divide the watt hours of the UPS by the maximum load the Snap Server draws. The result is the number of hours your UPS should supply power to maintain your Snap Server.

Registering your Server

To register your server, navigate to the **System > Registration** screen and click the **Register online now** link.



A separate browser window opens to a product registration form in which some of your product information is already entered. In addition, you may need to have the following information available:

- **Server number** — A numerics-only string
- **Serial number** — A 10-character alphanumeric string

These numbers appear on labels affixed to the inside of your Snap Server. To view the labels, remove the front bezel (4200, 4400, and 4500) or open the front door (14000).

Chapter 3

Networking Options

Snap Servers are preconfigured to use DHCP, autonegotiate network settings, and allow access to Windows, NFS, Macintosh, FTP, and Web clients. This chapter discusses your options for configuring TCP/IP addressing, network bonding, and access protocols. Network bonding options allow you to configure the Snap Server for load balancing and failover. Network protocols control which network clients can access the server.

- **Default Networking Configuration —** summarizes the default settings of each networking option.
- **Configuring TCP/IP —** discusses standalone, load balancing, and failover network bonding options and technical constraints in configuring TCP/IP addressing for single- or dual-Ethernet operation. Instructions and recommendations on using the Administration Tool to configure TCP/IP are also provided.
- **Managing Network Protocol Access —** provides instructions on how to configure the Snap Server to allow access to Windows, NFS, AFP (Macintosh), FTP, and Web clients.
- **Connecting from a Client —** provides instructions on connecting to the server via Windows, UNIX, Macintosh, FTP, and Web clients. Using the Web View screen is also discussed.

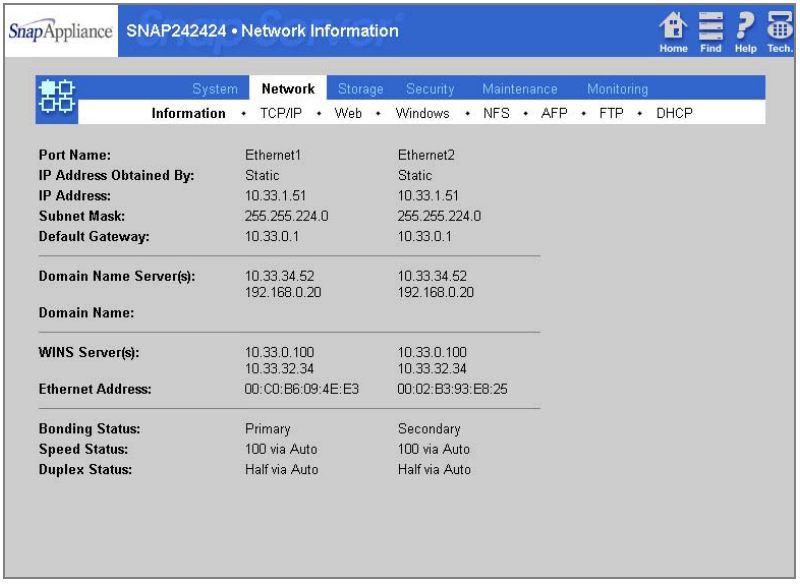
Default Networking Configuration

Snap Servers are preconfigured to allow multiplatform access in heterogeneous Windows, UNIX/Linux, and Macintosh environments. The following table summarizes the Snap Server's default networking configuration.

Protocol	Default	Comments
TCP/IP	**DHCP**	By default, Snap Servers acquire an IP address from the DHCP server on the network.
Network bonding	**Standalone**	*Network bonding* treats two ports as a single channel for failover or load balancing purposes. The *standalone* setting treats each port as a separate interface, effectively disabling network bonding.
Speed/duplex	**Auto**	The *speed* setting establishes the rate for transmission and reception of data. The *duplex* setting causes the Ethernet port to transmit packets in one way or two ways at the same time. The default setting of *Auto* enables automatic negotiation of the speed and duplex settings based on the physical port connection to a switch.
Windows (CIFS/SMB)	**Enabled**	Allows access to Windows clients via the workgroup domain.
NFS	**Enabled**	Allows universal access to all computers running NFS without client address restrictions.
Apple (AFP)	**Enabled**	Allows access over an Appletalk or TCP/IP network using the default zone.
FTP	**Enabled**	Allows read-only FTP access for anonymous users and read/write access for authorized users.
DHCP	Disabled	Allows Snap Servers to distribute IP addresses to network clients.
Require Authentication HTTPS	Disabled Disabled	Users can access files via HTTP using a web or file browser. Administrators may require users to log in to access files, and may also encrypt all traffic by enabling HTTPS.
SSH	Disabled	Required only when installing a supported backup agent or if you are troubleshooting under the direction of a technical support representative.

Configuring TCP/IP

The GuardianOS utilizes dual-Gigabit Ethernet technology to support standalone, load balancing, and failover network bonding modes. The following graphic displays the TCP/IP settings for a dual-Ethernet Snap Server in failover mode with autonegotiated speed and duplex settings.



Understanding Dual-Ethernet Bonding Options

Network bonding technology treats two ports as a single channel, with the network using one IP address for the server. To take advantage of network bonding, you need to have performed these operations: (1) both ports are physically connected to the network; (2) both ports are connected to the same switch on the same subnet.

Standalone

This mode (the default) treats each port as a separate interface. This configuration should only be used in multihomed environments in which network storage resources must reside on two separate subnets. Using this mode when both interfaces are connected to the same network segment is not supported and will lead to unexpected results.

Load Balancing

An Ethernet port on any server can become a bottleneck or single point of failure for a network. Using both Ethernet ports in a load balancing scheme increases server bandwidth and helps to keep users connected and files available.

In load balancing mode, the transmission load is distributed among aggregated network ports. An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses. This configuration enables the even distribution of network traffic across multiple network interfaces for optimal network performance.

Tip Load balancing can occur only on Layer 3 routed protocols (IP).

Failover

This mode uses the first Ethernet port as the primary network interface and the second Ethernet port is held in reserve as the backup interface. Redundant network interfaces ensure that an active port is available at all times. If the primary port (*Ethernet1*) fails due to a hardware or cable problem, the secondary port (*Ethernet2*) assumes its network identity.

The transition is transparent to users, although some may experience a few seconds of inactivity. If the failed port comes back online, it resumes its role as the primary interface. Failover mode ensures server availability to the network, but it does not provide switch fault tolerance.

Understanding Speed and Duplex Options

The Ethernet ports are capable of 10/100/1000 Mbps speeds, half/full- duplex, and autonegotiating configurations. The speed setting establishes the rate for transmission and reception of data. The duplex setting causes the Ethernet port to transmit packets in one way or two ways at the same time.

- **Half-duplex Ethernet —** Allows one-way transfer of data at a specified speed.
- **Full-duplex Ethernet —** Doubles the carrying capacity of a connection between two systems by allowing each system to simultaneously transmit and receive data. For example, a 100 Mbps/half connection allows 100 Mbps transfer speed in one direction at a time. A 100/full connection allows 100 Mbps transfer speed in both send and receive directions.

Busy networks that involve large file transfers between multiple clients benefit most from a full-duplex Ethernet, since they can send and receive traffic simultaneously from several clients.

Automatically Negotiating Speed/Duplex Settings

The automatic negotiation setting (*Auto*) allows the Snap Server to base speed and duplex settings on the physical port connection to a switch. When you use autonegotiation, the switch port must be configured to the same setting; otherwise, network throughput or connectivity to the server may be seriously impacted. Although high retransmission rates, collisions, or other errors sometimes demand lower throughput rate settings, such situations are best managed through hubs, routers, or switches rather than ports.

Tip Autonegotiation is the only allowable option for a Gigabit port.

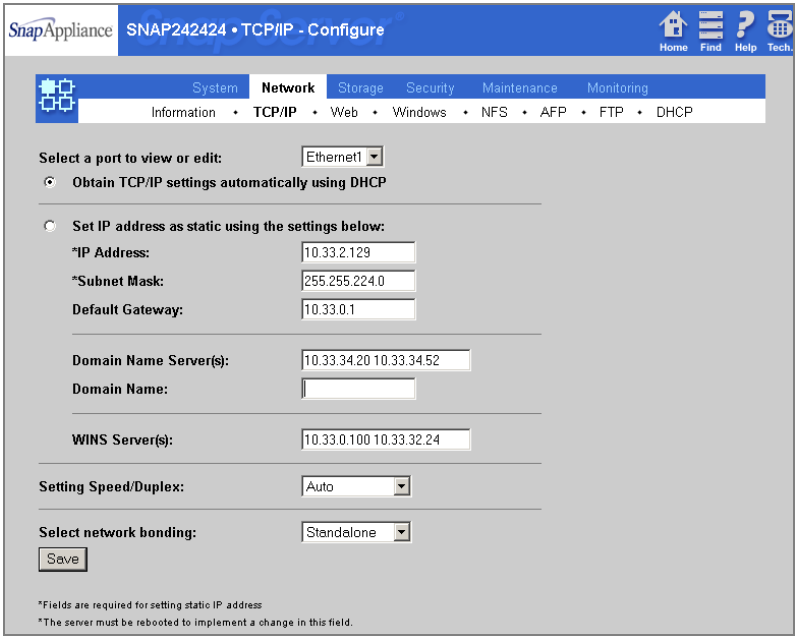
Restrictions on Shared-hub Configurations

The following restrictions apply to shared-hub configurations:

- You cannot employ full-duplex in a shared-hub configuration; shared hubs do not support full-duplex. You can employ full-duplex only when the Snap Server is connected to an Ethernet-switched port.
- You cannot implement Gigabit support in a shared-hub configuration. Attempting to force a Gigabit setting will have unintended consequences.

Configuring TCP/IP Settings

To change TCP/IP settings, navigate to the **Network > TCP/IP** screen. This screen defaults to the current settings for the primary Ethernet port (*Ethernet1*).



Edit settings as described in the following table, and then click **Save** to update network TCP/IP settings immediately. If you alter a static IP address or subnet mask, you may also need to reboot the server to activate those changes.

Option	Settings
Port	Select either *Ethernet1* or *Ethernet2* from the pull-down menu as appropriate. Note that the **Select Network Bonding** option appears only when Ethernet1 is selected.
TCP/IP Addressing	This defaults to the DHCP-assigned setting. To assign a static IP address, select **Set IP address as static using the settings below** and enter the following information: • IP address (required) • Subnet mask (required) Optionally, you may also specify the default gateway, domain name server, domain name, and WINS server as appropriate.
Speed / Duplex	Accept the default setting *Auto* to have the Snap Server automatically negotiate speed and duplex settings with the switch. This setting is recommended as the optimal solution for port settings, and *must* be selected to take advantage of a full-Gigabit connection. If you wish, you can also select a specific speed/duplex setting. If you manually configure speed/duplex settings, you must also configure the hub or switch with the same settings.
Network Bonding	This option appears only when *Ethernet1* is selected as the port. Choose one of the following settings: • *Standalone* provides two separate interfaces (one IP address per port). • *Failover* enables Ethernet2 to automatically take over the connection if Ethernet1 fails. Only one port is active at once. • *Load Balancing* enables both ports to share the transmission load while the primary port (Ethernet1) receives the traffic.

Managing Network Protocol Access

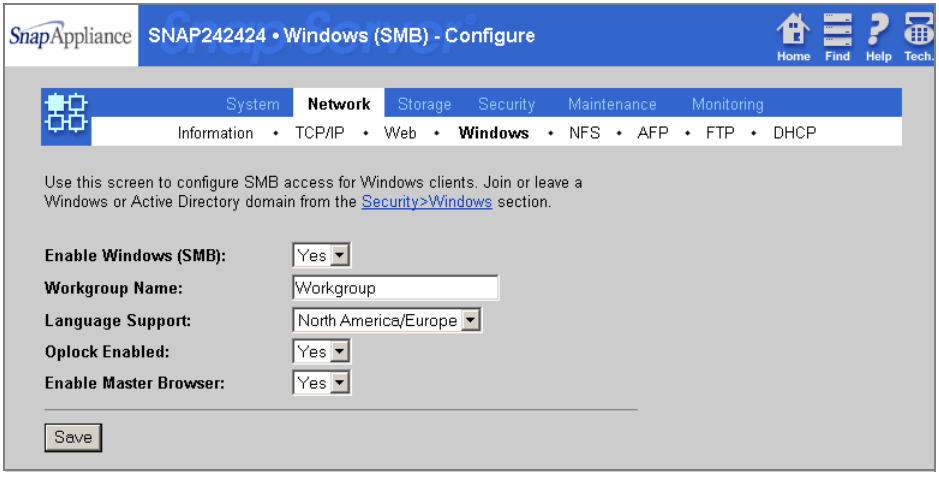
The Snap Server provides the standard file-sharing services of a Windows, NFS, Macintosh, HTTP, or FTP server. Users can access local server files, obtain read/write privileges to local server files, and share files with other clients. The Snap Server does not support other functions of these servers, such as printing or e-mail services.

This section shows you how to configure the Snap Server to accept Windows (SMB/CIFS), NFS, Macintosh (AFP), FTP, and Web (HTTP, HTTPS), clients. (For a complete listing of supported file protocols and client types, see "Snap Server Specifications" on page 147.) You can also configure a Snap Server to act as a DHCP server.

Tip For security reasons, many administrators prefer to disable any protocols that are not in use on their networks.

Configuring Windows Access

To change Windows settings, navigate to the **Network > Windows** screen. The default settings make the Snap Server available in the workgroup named 'Workgroup'.

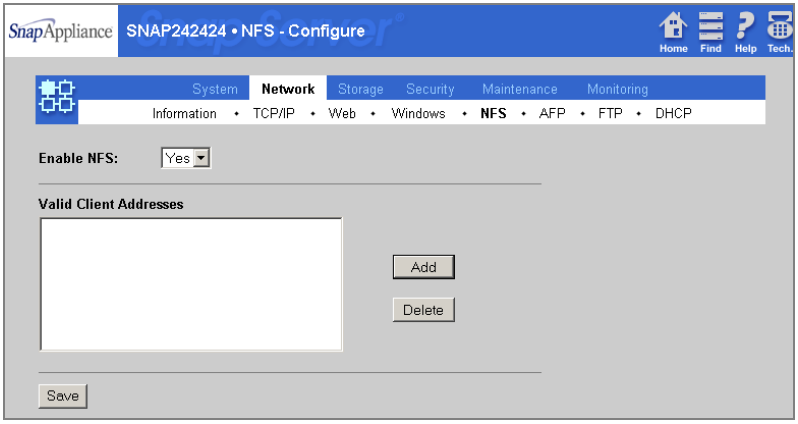


Edit settings as described in the following table, and then click **Save** to update Windows network settings immediately. For information on security and authentication, see "Security Management" on page 73.

Option	Settings
Workgroup/Domain	This defaults to the Windows workgroup. Enter the workgroup or domain name to which the server belongs. If you join a Windows domain through Advanced Security (**Security > Windows**), the domain name you entered displays here and can be changed only via the Advanced Security screen.
Language Support	In the Language Support field, select the code page used by Windows clients when they transmit file and folder names in a single-byte character set: • *North America/Europe* refers to code page 850 (Western Europe including Afrikaans, Basque, Catalan, Dutch, English, French, German, Italian, Indonesian, Icelandic, and Spanish). • *United States* refers to code page 437 (US English, Indonesian, Basque, Catalan). • *Nordic/Europe* refers to code page 865 [Northern Europe including Danish, Finnish, Norwegian (Bokmål), Norwegian (Nyorsk), and Swedish]. The Snap Server supports the primary Icelandic code page (865), but does not support the secondary page (861).
Opportunistic Locking (Oplock)	If desired, select *Yes* to enable opportunistic locking. Oplock can help performance if the current user has exclusive access to a file.
Enable Master Browser	The Snap Server can maintain the master list of all computers belonging to a specific workgroup. (At least one Master Server must be active per workgroup). Select *Yes* if you plan to install this server in a Windows environment and you want this server to be able to serve as the Master Browser for a workgroup.

Configuring NFS Access

To change NFS access, navigate to the **Network > NFS** screen. The Valid Client Addresses list box displays the client machines that currently have access to the server via NFS.

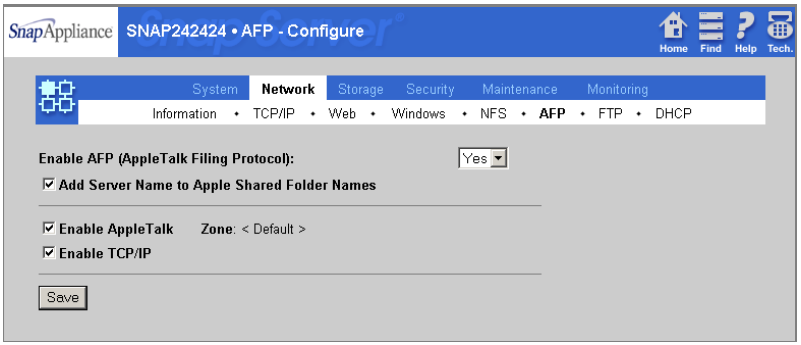


Edit settings as described in this section, and then click **Save** to update NFS network settings immediately. For information on security and authentication, see "Security Management" on page 73.

Type of Access	Procedure
Universal Access	Universal access eliminates validation, and grants access to all NFS connections. 1 Make sure the Valid Client Addresses list box is blank. 2 If necessary, select one or more entries and click **Delete**.
Access to specific clients	1 Click **Add**. 2 In the Valid Client Addresses field, enter one client IP addresses. (In an environment with name resolution, you can enter a host name as well.) 3 When finished, click **OK**. The client address appear in the list box. 4 To add more addresses, repeat steps 1 through 3.

Configuring Apple File Protocol (AFP) Access

To change AFP settings, navigate to the **Network > AFP** screen. The default settings provide access to Macintosh clients over an AppleTalk or TCP/IP network.



Edit settings as described in the following table, and then click **Save** to update network AFP settings immediately.

Options	Usage
Adding the Server Name to Apple Shared Folder Names	Select the **Add Server Name to Apple Shared Folder Names** option to show both the server name and share name in the Select a File Server dialog box. Clear the check box to display only the share name.
AppleTalk Networking	Select the Enable AppleTalk check box to enable access across an AppleTalk network. Clear the check box to deny access to AppleTalk network clients.
Zone	The Snap Server scans its local subnet for the presence of an AppleTalk router, and adjusts the behavior of this field accordingly: • If an AppleTalk router is detected, a pull-down menu displaying the available zones appears. Choose one of the following options: a) leave the field blank to use the default zone; or, b) select the appropriate zone from the pull-down menu. Using the default zone ensures proper coordination among multiple Snap Servers on the same subnet and provides greater compliance with third-party software. • If an AppleTalk router is not detected, the text string < Default > displays.
TCP/IP Networking	Select the **Enable TCP/IP** check box to enable AFP over TCP/IP. Clear the check box to disable AFP over TCP/IP.

Configuring FTP Access for Anonymous Users

To change FTP settings for anonymous login, navigate to the **Network > FTP** screen. The default settings allow read-only access for anonymous users, and read/write access for authorized users. Edit settings as described in this section, and then click **Save** to update network FTP settings immediately.

Option	Settings
Anonymous Login	When you allow anonymous login, FTP users employ an e-mail address as the password. When you disallow anonymous login, only FTP users who are configured as local Snap Server users can access the server. Select one of the following access options from the pull-down menu: • *Read Only* means anonymous users who log in through FTP anonymously have read-only privileges. • *Read/Write* means anonymous and authenticated users have read/write privileges. • *No* means users cannot log in anonymously, but must instead log in via their own local user name, password, and access permissions.

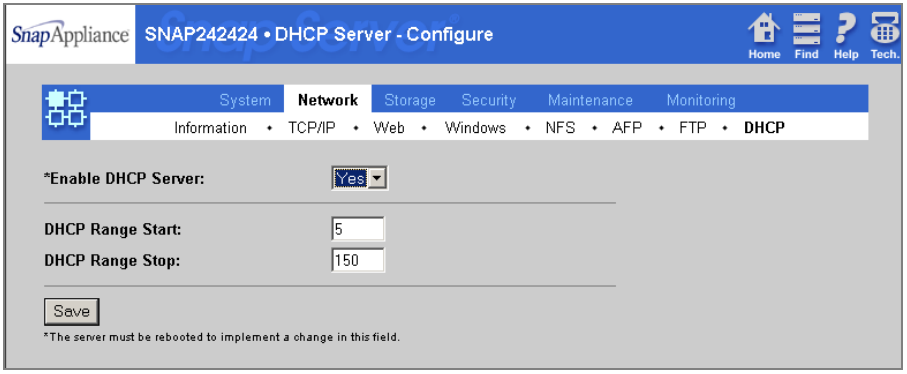
Configuring a DHCP Server

To configure the Snap Server as a DHCP server, it must have a static IP address. This static address must meet two conditions: (1) it must lie outside the DHCP range of IP addresses you specify on the DHCP screen; and, (2) it must be part of the same subnet on which the Snap Server is to assign IP addresses. You can assign the Snap Server a static IP address on the **Network > TCP/IP** screen.

Caution Ensure that the network has no other active DHCP servers. You may negatively impact the network if you enable this device as a DHCP server while another server on the network is performing this function.

To enable the Snap Server as a DHCP server, follow this procedure:

1 Navigate to the **Network > DHCP** screen, and select *Yes* from the pull-down menu.



2 Configure the range of IP addresses from which the server will choose. Enter values for DHCP Range Start and DHCP Range Stop. For example, suppose the Snap Server has a static IP of 192.168.0.2 on a subnet mask of 255.255.255.0.

Entering 5 in the Start field and 150 in the Stop field produces the following DHCP range:

192.168.0.5 to 192.168.0.150.

3 Click **Save**.

When you enable the Snap Server as a DHCP server, it reports in-use IP addresses at the bottom of the screen under Current DHCP Status.

Connecting from a Client

A Snap Server, once installed, appears on the network as a server with a shared folder.

Windows (SMB)

Windows clients can connect to the Snap Server using either the server name or IP address. To navigate to the server using Windows Explorer, use one of these procedures:

- For Microsoft Windows 2000, Me, or XP clients, navigate to **My Network Places >** *workgroup_name* > *server_name*.
- For Microsoft Windows 95, 98, or NT clients, navigate to **Network Neighborhood >** *workgroup_name* > *server_name*.

Unix/Linux (NFS)

A share on a Snap Server is equivalent to an exported file system on an NFS server. NFS users can mount Snap Server shares and access content directly, or mount a subdirectory of a share, using the following procedure:

1 From a command line, enter the following command:

```
mount server_name:/share_name  /local_mount
```

where *server_name* is the name or IP address of the server, *share_name* is the name of the share you want to mount, and *local_mount* is the name of the mount target directory.

2 Press Enter to connect to the specified share on the server.

Macintosh (AFP)

Some Snap Server terms may cause confusion for those familiar with Apple terminology. For example, share terminology differs. Each Snap Server share (or shared folder) appears as a Macintosh volume that can be accessed through the Chooser. Unlike standard AppleShare servers, the Snap Server allows *nested* shares (shared folders within shared folders). As a result, it is possible for some files or directories to appear in more than one shared folder.

Share names are also handled differently. By default, the Chooser identifies Snap Server shares using only the share name. To display both the share name and the server name, enable the **Add Server Name to...** check box on the **Network > AFP** screen. This strategy allows Macintosh applications to differentiate between shared folders with the same share name on multiple servers. For example, SHARE1 on SNAP61009 refers to the share named SHARE1 on the Snap Server named SNAP61009.

Tip You must add Macintosh networking users and groups as local Snap Server users and groups.

To Connect to the Snap Server from a Macintosh, use this procedure:

1. Select **Network Browser**, **Chooser**, or **Connect to Server** from the Apple or GO menu. In the Chooser, click the **AppleShare** icon.
2. If using zones with AppleTalk, select the default zone in the AppleTalk Zones list.
3. Scroll through the list of servers in the Select a File Server list and select your server, then click **OK**. (In Mac OS X, you may need to enter the IP address of the server.)
4. When asked for a user name and password, enter them (or click **Guest**), then click **OK**.
5. In the Server dialog box, select the shared folder you want to mount on your desktop, and click **OK**.

Tip For Mac OS X, you can also mount via NFS, as described in "Unix/Linux (NFS)" on page 49.

FTP

To connect to the server through FTP, use the following procedure. Note that users cannot manage files or folders in the FTP root directory.

Tip Only locally defined users can connect via FTP. For information on creating local users, see page 78.

1. Enter the server's name or IP address in the FTP Location or Address box.
   - To connect via a command line, enter ftp *server_name*
   - To connect via a Web browser, enter ftp://*server_name*

   where *server_name* is the name or IP address of the server.
2. Enter a valid user name and password to log in. If access to a share is restricted, users must log in with the correct privileges to browse the contents of the share.
3. Press Enter to connect to the FTP root directory. All shares and subdirectories appear as folders.

Web Browser (HTTP)

Users can view and download files using a browser, but cannot modify or upload files. To access a specific share directly, Internet users can append the full path to the Snap Server name or URL, as shown in the following examples:

```
http://SNAP61009/Share1/my_files
```

```
http://10.10.5.23/Share1/my_files
```

Tip Web access is case-sensitive. Capitalization must match exactly for a Web user to gain access.

To Connect Using a Web Browser

Access the server using either of the supported browsers: Microsoft Internet Explorer (4.0 or better), or Netscape Navigator (4.7x or better).

1. Enter the server name or IP address in the browser. (The default server name is SNAP*nnnnnn*, where *nnnnnn* is the server number.)
2. Press Enter. The Web View screen opens.

Web View is the screen that opens when users access a Snap Server using their Web browsers. Web View displays a list of all shares. (Shares designated as *hidden* will not be visible to Windows, Macintosh, or Web browser users from Web View. For more information, see "Setting Share Access Permissions" on page 85.)

Using the Web View screen

- **Requiring users to log into Web View —** By default, Snap Servers permit anonymous login. To enable HTTP authentication, navigate to the **Network > Web** screen, select *Yes* in the Require Web View Authentication field, and click **Save**.

Chapter 4

Storage Configuration and Management

Storage configuration consists of selecting the type of RAID appropriate to your user requirements, setting up one or more volumes (file systems) for the RAID, and defining access to those file systems via shares. This chapter explains the default storage configuration, how to create a different configuration, and how to monitor and maintain the health of storage components.

- **Default Storage Configurations** — Summarizes the default storage settings for the Snap Servers
- **Snap Server Storage Configuration Options** — Defines the RAID configurations available on the Snap Server; discusses concepts in volume management, including the Snapshot pool and quotas; and lists the types of shares.
- **Creating New Storage Configurations** — Provides instructions on creating new RAIDs, volumes, and shares.
- **Managing and Repairing RAIDs** — Discusses how to recognize and replace failed disk drives.
- **Managing Volume Usage** — Discusses how to monitor and control volume usage by establishing usage quotas for users and groups.
- **Hot Swapping Disk Drives** — Provides information on how to physically replace disk drives on Snap Servers.

Default Storage Configurations

Snap Servers are preconfigured as a single RAID 5, with a single volume encompassing the entire RAID, and a single share pointing to the volume. The data space is preconfigured to allocate 20 percent of the RAID to Snapshots on the single volume and the remainder of the RAID for the file system.

- The Snap Server 4200, 4400, or 4500 is a 4-disk RAID 5 with no hot spare
- The Snap Server 14000 is an 11-disk RAID 5 and one hot spare

The following table provides details on the Snap Server's default storage configuration.

Component	4200-4500	14000	Comments
RAID	4-Disk RAID 5	11-Disk RAID 5	*RAID* refers to a collection of disk drives that act as a single storage system.
Hot spare	Not configured	Yes	A *hot spare* is a disk drive that can automatically replace a damaged drive.
Snapshot pool	(20%)	(20%)	A *Snapshot* is a consistent, stable, point-in-time image of a volume (file system) used for backup purposes. Snapshots are stored on the RAID in a *Snapshot pool*, or space reserved on the RAID for this purpose.
Volumes	1	1	A *volume* is a logical partition of a RAID's storage space that contains a file system. The default volume (VOL0) organizes the remaining RAID capacity (after the Snapshot pool) into a single storage space with a single file system.
Shares	1	1	A *share* is a virtual folder that maps to the root of a volume or a directory on the volume. The default share (SHARE1) maps to the root of the volume. The *share access* settings of the default share grant access to all users and groups over all protocols.
Snapshot shares	None	None	A *Snapshot share* is a virtual folder that allows access to all current Snapshots at the same directory level as the original share on which it is based.
Quotas	Disabled	Disabled	A *quota* is a limit on the amount of storage space on a volume that a user or NIS group can consume.
Directories	None	None	If desired, you can use the Administration Tool (**Storage > Directories**) to create a volume's directory structure.

Storage Configuration Options

The default storage configurations offer high levels of data security and storage capacity with a minimum of maintenance overhead. If the default configuration is appropriate to your needs, the only further storage configuration necessary is creating the directory structure, establishing share access to the directories, and setting up Snapshots.

You may have requirements or special needs that demand a different configuration. For example, if the information on a Snap Server is mission-critical but infrequently accessed, creating a RAID 1 with a hot spare could be a justifiable option. In another example, some administrators prefer to keep certain sensitive data, such as financial records, in a separate file system for added security.

This section defines your options for configuring storage on a Snap Server, and brings to your attention dependencies that you should consider before designing and implementing a new storage configuration.

RAIDs

The type of RAID configuration you choose depends on a number of factors: (1) the importance of the data; (2) performance requirements; (3) drive utilization; and, (4) the number of available drives. For example, in configuring the four disk drives of the 4500, the decision whether to include a hot spare in the RAID depends on the value you place on capacity vs. availability. If capacity is paramount, you would use all drives for storage; if high availability were more important, you would configure one of the drives as a hot spare. The following table summarizes the advantages and disadvantages of each type of RAID:

	RAID 0	RAID 1	RAID 5
Data loss risk	high	lowest	low
Write access speeds	fast	slower	fast
Cost/MB	lowest	high	low
Disks required	1 or more	2 or more	3 or more
Accepts hot spares?	no	yes	yes

RAID 0 (Striped)

RAID 0 distributes data evenly among all disks in the array. This technique, called *data striping*, results in fast access speeds since it uses multiple physical devices to store the data. However, RAID 0 offers no redundancy, and does not accept hot spares. If a single disk drive fails, every file in the RAID is rendered unavailable.

RAID 1 (Mirrored)

RAID 1 uses mirroring, which stores data on one disk drive and copies it to another drive in the RAID. A RAID 1 must contain at least two disk drives: one for the data space and one for redundancy. Though the data space in a RAID 1 can never be larger than a single drive, some administrators prefer to add a third drive (either as a hot spare or a member) for additional redundancy. RAID 1 is the most secure method for storing mission-critical data because there is no catastrophic data loss when a disk fails. However, RAID 1 is the most expensive and least efficient storage method.

RAID 5 (Striping with Parity)

RAID 5 distributes data evenly among all disks in the array, and maintains parity information (error correction data) that allows the system to recover from a single disk drive failure. RAID 5 provides the best combination of performance, usability, capacity, and data protection.

Hot Spares

A *hot spare* is a disk drive that can automatically replace a damaged drive in a RAID 1 or 5. If one disk drive in a RAID fails the RAID automatically uses the hot spare to rebuild itself without administrator intervention.

Volumes

The default configuration organizes the remaining RAID capacity into a single volume with a single file system. If you need separate file systems on the same server, you can delete the default volume and create two or more smaller volumes in its place.

As previously noted, the default RAID capacity is divided between the Snapshot pool (20%) and the volume (80%). You can increase or decrease Snapshot pool size at any time; you can increase, but not decrease the size of a volume.

- If a pool reserve of 20% is more than you require, you can decrease the pool size, then add the freed space to the volume.
- If you find you need to reserve more than 20%, you will have to delete the volume, expand the pool size, and then create a new volume.

Snapshot Pool Size

The default configuration reserves 20 percent of the volume's capacity for the Snapshot pool. You may need to adjust this figure depending on your Snapshot strategy, write activity, and other factors. For more information, see "Managing the Snapshot Pool" on page 99.

Shares

A Snap Server share may be thought of as equivalent to a Microsoft networking share, a Macintosh networking shared folder, or an NFS exported file system. The default share provides all users unrestricted access to the entire volume over all supported protocols.

Share access security allows administrators to assign read-write or read-only access to users and groups within a share. Access to share can also be restricted by disabling protocols.

Administrators may also conceal a share from users accessing the Snap Server over certain protocols. A *hidden* share is one that restricts the display of the share via the Windows (SMB), Web View (HTTP/HTTPS), and Apple (AFP) protocols. For more information, see "Setting Share Access Permissions" on page 87.

Snapshot Shares

A Snapshot share provides access to all current Snapshots of a volume. Just as a share provides access to a portion of a live volume, a Snapshot share provides access to the same portion of the file system on any archived Snapshots of the volume. You create a Snapshot share by selecting the **Create Snapshot Share** option in the course of creating a live-volume share. For more information, see "Creating a Share" on page 62.

Creating New Storage Configurations

The Snap Server offers two methods of creating a new storage configuration: (1) the RAID Storage wizard lets you quickly create a RAID, a volume to the RAID, and a single share to the volume; or, (2) a sequence of Storage screens requires a little more time, but allows you full control over volume, share, and share access definitions. The wizard is the fastest way to create a RAID, but the Storage screens offer more choices and greater flexibility.

Before You Begin

Before you can create a new storage configuration, you must delete the default configuration. If you have already begun using your Snap Server, you must back up all data before you reconfigure a RAID or a volume. Before creating a new storage configuration, consider the following:

Caution Deleting a RAID (or a volume) deletes all data stored on its disk drives. (Deleting a share does not delete any data.)

- **The RAID type is appropriate and scalable to your users' needs —** Determine the type of RAID you want to create, and make sure the server has enough unassigned disk drives for the configuration (including a hot spare, if any). You cannot grow a RAID. If you later decide the RAID requires more space, you must back up the data, delete the RAID, create a new one, and then restore the data.
- **The volume capacity is properly sized, including enough space to accommodate your Snapshot strategy —** Once created, a volume can be enlarged but not reduced in capacity. If you plan to use Snapshots, you must set aside space on the new volume for this purpose. See "Snapshot Storage" on page 87 for more information on estimating Snapshot space requirements.
- **You cannot create a directory during the share-creation process —** Before creating a share, make sure the directory to which the share will point exists, and you know its name, volume, and path.
- **If you are using Backup Express for GuardianOS, preserve the catalog file —** The catalog (a Backup Express for GuardianOS file that keeps track of the data you back up) resides on the default volume. If you delete this volume (and it is the last available volume), the catalog is also deleted. To retain catalog information, you must back up the catalog (see page 112) before you delete the volume, create your new storage configuration, and then restore the catalog.
- **The *e*Trust Inoculate*IT* software may be deleted —** The antivirus software is installed and enabled on the default volume. Deleting this volume (if it is the last available volume) also deletes the antivirus software. After creating your new storage configuration, you can reinstall the software by navigating to the **Maintenance > Antivirus** screen, selecting *Yes*, and clicking **Save**. The Snap Server

reinstalls the antivirus software (using default settings) on the largest volume. The installation process does not preserve custom antivirus configuration settings. Make a note of any such settings before deleting a RAID or volume.

Using the RAID Storage Wizard

To create a storage configuration with the RAID Storage Wizard, navigate to the **Storage > Wizard** screen. The wizard walks you through the storage configuration process.

Tip Each RAID type requires a minimum number of available drives. A RAID type will only be available if its minimum drive requirement is met.

1. **Select a RAID type.**

   To start the wizard, click the RAID type you want to create. A list of available disk drives appears.

2. **Select drives.**

   Select the drives for the RAID from the list provided. If you are creating a RAID 1 or RAID 5, you can configure one of the selected drives as a hot spare by selecting the **Add Hot Spare** check box. Click **Continue** to confirm your RAID configuration.

3. **Create the RAID.**

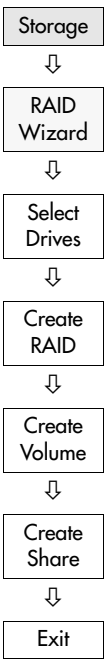
   Review the information on this screen to verify the RAID configuration, and then click **Continue** to open the Create Volume screen.

4. **Create a volume.**

   The volume capacity defaults to the entire storage space of the RAID. You can enter a lesser number if you plan to create additional volumes on the RAID, or you need to reserve some space for the Snapshot pool. Click **Continue** to create the volume and open the Create Share screen.

5. **Create a share to the volume.**

   Make a note of the share name and click **Continue** to create a share that allows access to all users via all protocols. (You can modify the share access definition by navigating to the **Security > Shares** screen, and clicking the name of the share.)



Creating a RAID

To create a new RAID, navigate to the **Storage > RAID** screen. Creating a RAID involves choosing the RAID type, selecting the disk drives to include in the RAID, and then creating the RAID. When finished, you can continue to the Create Volume screen or exit to the RAID Sets screen.

Tip Each RAID type requires a minimum number of available drives. A RAID type will only be available if its minimum drive requirement is met.

1 **Select the RAID type.**

To start the process, click **Create RAID Set**. On the screen that opens, choose the type of RAID you want from the pull-down menu. Click **Continue** to view a list of unassigned drives.

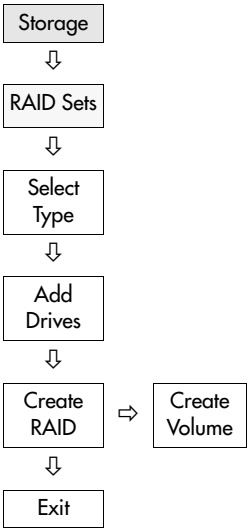
2 **Select the disk drives.**

If you are creating a RAID 1 or RAID 5, you can configure one of the selected drives as a hot spare by selecting the **Add Hot Spare** check box. (This check box becomes active after you have selected the minimum number of drives required for the RAID.) Click **Continue** to confirm your configuration.

3 **Create the RAID.**

Review your settings and click **Continue** to create the RAID. On the confirmation screen, do one of the following:

- To create a volume for the new RAID set, click **Create Volume**.
- To return to the RAID screen, click **Exit**.

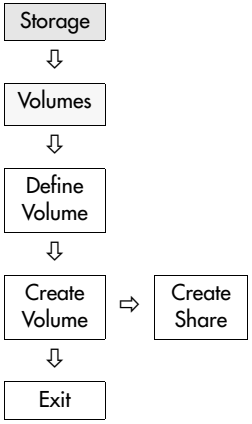


Creating a Volume

To create a volume, navigate to the **Storage > Volumes** screen. Creating a volume is a simple process of defining the name, location, and size of the volume. When finished, you can continue to the Create Share screen or exit to the Volumes screen.

1 **Define the volume.**

To begin the process, click **Create Volume**. On the screen that opens, define the volume's parameters:



- If necessary, select the RAID on which to create the volume. The screen refreshes to display the options and information appropriate to the RAID Set's remaining capacity.
- Accept the default volume name, or enter a new one. To rename the volume, use up to 20 alphanumeric characters, including the hyphen, but starting with an alphanumeric character.
- The capacity of the volume defaults to the total remaining capacity on the RAID set. If you plan to have only one volume on the RAID and do not plan to use Snapshots, accept the default value. If you plan to have more than one volume, or you need to reserve space for the Snapshot pool, adjust the value accordingly.

2 **Create the Volume.**

Review your settings and click **Continue** to create the volume. On the confirmation screen, do one of the following:

- To create a share for the new volume, click **Create Share**.
- To return to the Volumes screen, click **Exit**.

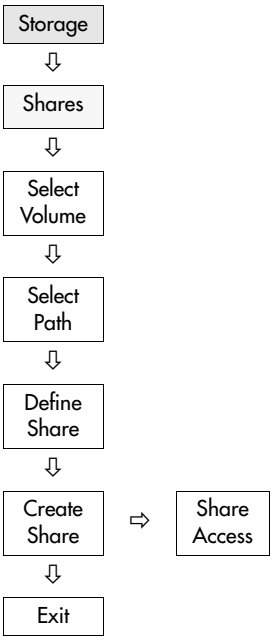
Tip When you create a new volume, make sure you create a share to the root of the volume. This share is important for backup purposes.

Creating a Share

To create a share, navigate to the **Storage > Shares** screen. Creating a share involves selecting the volume and directory path for the share and then defining share attributes and network access protocols. Before you start, make sure you know the name, volume, and path to the directory to which the share will point.

1 **Select a volume.**

To begin the process, click **Create Share**. On the screen that opens, choose the volume you need from the pull-down menu, and then click **Continue**.



2 **Select the path to the directory.**

The Current Path field defaults to the root path of the volume.

- To create a share to the entire volume, simply click **Use Current Path**.
- To create a share to a directory, navigate to and select the directory in the Select a Different Path area, then click **Use Current Path**.

The Share Definition screen opens.

3 **Define the share.**

Use this screen to enter the following:

- Accept the default share name, or enter a new one. If you change the default, make sure the name is unique.
- If desired, enter a description of the share. This text appears in Web View.
- To create a create a share to archived Snapshots of the volume, select the **Create Snapshot Share** check box. Accept the default name or enter a new one. (For more information on Snapshots and Snapshot shares, see page 98.)
- Select the access protocols for the share: Windows (SMB), Web View (HTTP), NFS, Apple (AFP), and FTP.

Click **Continue** to review your selections.

4 **Create the share.**

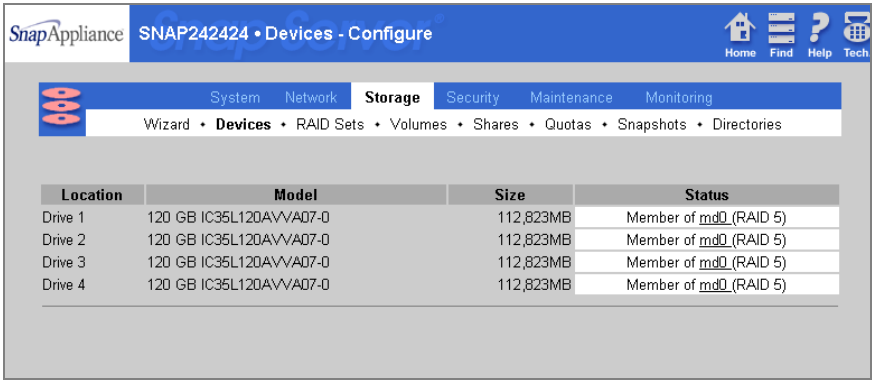
Review your settings and click **Continue** to create the share. On the confirmation screen, do one of the following:

- To set access permissions for the share, click **Set Share Access**.
- To return to the Shares screen, click **Exit**.

Managing and Repairing RAIDs

Determining Disk Drive Status

To view the status of the disk drives installed on the server, navigate to the **Storage > Devices** screen.



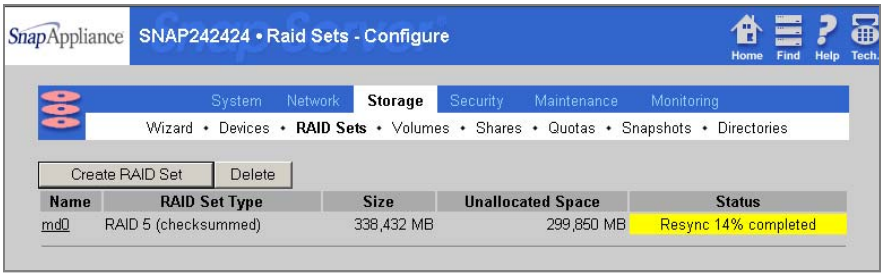
The devices table displays the location, model, and capacity of each drive. The status of each drive is indicated as follows:

- **Member of...** — The RAID set to which the drive is assigned
- **Unassigned** — Not a member of any RAID
- **Hot spare** — The drive is reserved as a hot spare
- **Failed** — The drive is offline or otherwise inaccessible
- **Empty** — The drive slot does not contain a drive

Tip In the Status column, you can click the name of a RAID to view the RAID's configuration.

Determining RAID Set Status

To assess the status of a RAID, navigate to the **Storage > RAID Sets** screen. Conditions that may require your attention are highlighted in yellow.



The RAID table displays the name, type, total capacity (size), and the remaining capacity not allocated to a volume for each RAID. RAID status is indicated as follows:

- **OK** — The RAID is functioning properly.
- **Degraded** — A drive has failed or been removed.
- **Resync** — A RAID repair operation is in progress.
- **Failure** — The RAID Set is off-line.

Tip You can set the E-mail Notification feature to alert you when a RAID degrades. See "Configuring E-mail Notification" on page 122.

Replacing Disk Drives on a RAID

This section describes how to safely remove and add drives to a degraded RAID. On Snap Servers, a drive must be removed logically from the RAID using the Administration Tool before it is removed physically from the server. Likewise, after a fresh drive is inserted into the drive bay, you must use the Administration Tool to add it to a RAID.

How RAIDs React to Disk Drive Removal

- **RAID 0** (nonredundant) — Removing a disk drive from a RAID 0 causes the RAID to fail. This action renders any data residing on its drives inaccessible, and is not recommended. If a RAID 0 disk drive is inadvertently removed, reinserting it should restore file access.
- **RAID 1 or 5** (redundant) — Removing a disk drive from a RAID 1 or RAID 5 places the RAID into degraded mode. While operating in a degraded mode, users can access or even update data. However, the array loses its redundant characteristics until all drives of the array are available and operating properly.

Tip If you configure a RAID 1 or 5 with a hot spare, the array automatically starts rebuilding with the hot spare when one of the disk drives fails or is removed.

To Replace a Disk Drive

The following procedure assumes that you are installing a new, out-of-the-box disk drive as a replacement for a failed drive.

1. **Remove a disk drive logically from an existing RAID using the Administration Tool.**

   Navigate to the **Storage > RAID Sets** screen. Click the name of the RAID that contains the failed drive to view the RAID's Edit screen. In the Actions column, click the failed drive's **Remove** link. On the confirmation screen, click **Continue**. You return to the RAID's Edit screen. The RAID status now reads *Degraded*.

2. **Physically remove the failed disk drive, and insert a new one in its place.**

   See page 70 for detailed instructions on physically replacing a disk drive. After the drive is removed, navigate to the **Storage > Devices** screen. The status of the new drive now reads *Unassigned*.

3. **Add the disk drive logically to a degraded RAID using the Administration Tool.**

   Navigate to the **Storage > RAID Sets** screen and click the name of the degraded RAID. On the RAID's edit screen, click **Repair** to view a list of available drives. Select a drive from the list, and click **Continue**. On the confirmation screen, click **Continue**. You return to the RAID's Edit screen. The status of the RAID now reads *Resyncing*, and the status of the newly added drive shows as *Hot Spare*.

Adding Disk Drives to a RAID

This section describes how to safely add drives to an existing RAID 1 or 5. On Snap Servers, after a fresh drive is inserted into a drive bay, you must use the Administration Tool to add it to a RAID.

How RAIDs React to Disk Drive Additions

- **RAID 0** (nonredundant) — You cannot add a drive to a RAID 0. To reconfigure a RAID 0, you must delete the RAID and recreate it.
- **RAID 1** (redundant) — You can add a new drive to a RAID 1 as either a hot spare or as a new member. Adding a disk drive to a RAID 1 does not add storage capacity. The new drive simply creates an additional copy of the original drive.
- **RAID 5** (redundant) — You can only add a hot spare to a RAID 5; you cannot add a new drive as a new member to an existing RAID 5.

To Add a Drive to an Existing Raid 1 or 5 Using the Administration Tool

1. Navigate to the **Storage > RAID Sets** screen, and click the name of the RAID 1 or 5 to which you want to add a drive.
2. On the screen that opens, click **Add**. If you are adding to a RAID 1, select either **Hot Spare** or **Member** at the top of the screen. (Adding a member is not available for a RAID 5.)
3. Select one or more drives to add to the configuration, and then click **Continue**.
4. On the confirmation screen, click **Continue**.

To Reintegrate Orphaned Disk Drives

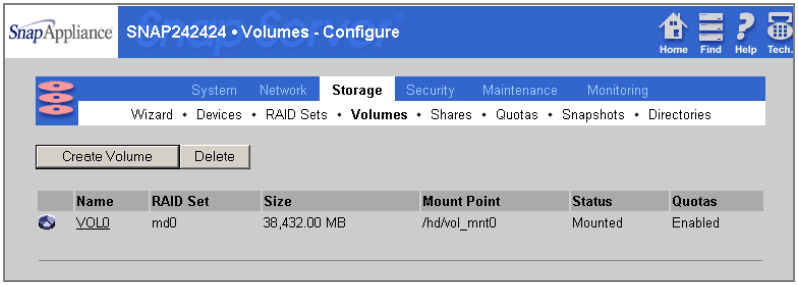
An *orphan* disk drive occurs in the following circumstances: (1) a working drive from a RAID is accidentally removed from the server; (2) the RAID or system is started with a drive missing; or, (3) a drive in a RAID intermittently fails, then appears to work again. The server cannot distinguish between the accidental removal and the intermittent failure. In either case, the drive becomes suspect and is considered an orphan. To remedy the problem, add the drive using the procedure just described.

Managing Volume Usage

The Snap Server offers several tools for monitoring and controlling how storage space on a volume is used. You can dynamically grow and manipulate volumes without rebooting the server.

Assessing Volume Status

To view information on existing volumes, navigate to the **Storage > Volumes** screen.



The volumes table displays the name, RAID, total capacity (size), and mount point for each volume. The status of each volume is indicated as follows:

- **Mounted** — The volume is online and accessible.
- **Not mounted** — The volume is offline.
- **Rollback** — A Snapshot rollback operation is in progress.

The table also displays whether quotas are enabled or disabled.

Using Quotas to Control Volume Usage

A quota is a limit on the amount of storage space on a volume that a user or NIS group can consume. Assigning quotas ensures that no one user or group consumes an excessive amount of volume space. In addition, quotas keep tabs on how much space each user or group is currently consuming on the volume, allowing for precise tracking of usage patterns.

You can set individual quotas for any local, Windows domain, or NIS user known to the Snap Server. Group quotas are currently available only for NIS groups. When you add a user to the quota table, the quota defaults to 100 MB; for a group, the default is 1000 MB. Quotas may range from 1 MB up to the total capacity of the volume.

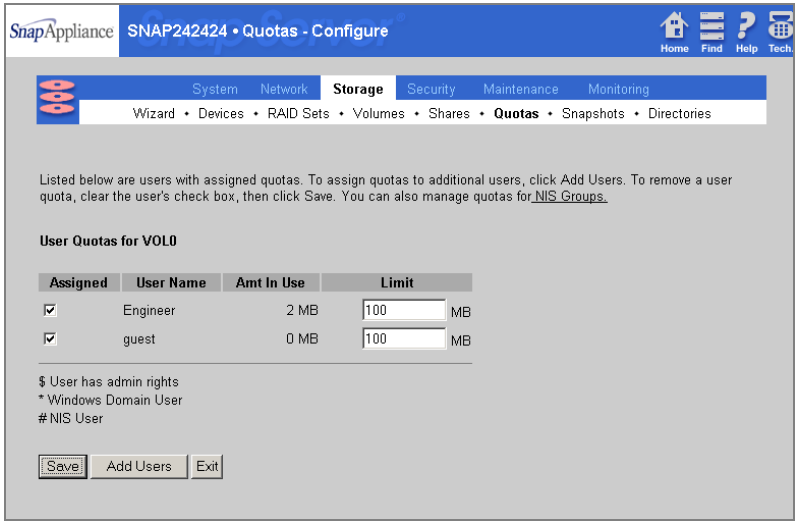
In calculating usage, the Snap Server looks at all the files on the server that are owned by a particular user, and adds up the file sizes. Every file is owned by the user who created the file and by the primary group to which the user belongs. When a file is copied to the server, its size is applied against both the applicable user and group quota.

Assigning User or Group Quotas

To assign quotas, navigate to the **Storage > Quotas** screen. Assigning quotas involves enabling quotas for a volume, adding users or NIS groups to one of the volume's two quota tables, and then setting a limit (in MB) on the amount of space each user or group can consume.

1 **Enable quotas for the volume.**

A check mark in the Enabled column indicates that quotas for a volume are enabled. To enable quotas for a volume, select its check box and click **Save**. Then select the volume name to view its current user quota table.



2 **Access the users or group quota tables.**

If you plan to assign user quotas, proceed to step 3. If you plan to assign NIS group quotas, click the **NIS Groups** link in the introductory text.

3 **Add or remove accounts, and assign quotas.**

You use the quota table screens to: (1) add and remove user or group accounts from the table; and, (2) assign quotas.

- **To assign a quota**, enter a number in the Limit column. Quotas may range from 1 MB up to the total capacity of the volume
- **To add a user or group to the table**, click the appropriate **Add** button to view a list of all users (or all groups) known to the server. Find the accounts you want by browsing or searching the list. After selecting all the accounts you need, click **OK** to transfer them to the quota table. Finally, click **Return** to go back to the quota table screen.

- **To remove a user or group from the table**, clear the check box(es) in the Assigned column.

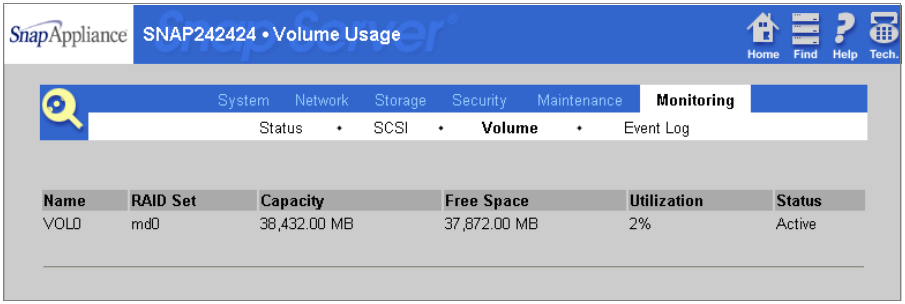
4 Click **Save**. Any changes you have made take effect immediately.

Disabling Quotas

To disable quotas, clear a volume's check box in the Enabled column and click **Save**. Disabling quotas for a volume deactivates any existing quota assignments you have made, but does not delete them.

Tracking Volume Usage

To view the current utilization totals for each volume, navigate to the **Monitoring > Volume** screen.



The volume usage table displays the name, RAID, and status for each volume. Usage is presented as follows:

- **Capacity —** The total storage space available in the volume
- **Free space —** The amount of unused storage space remaining in the volume
- **Utilization —** The percentage of total volume capacity in use, calculated by dividing free space by capacity

You can use the **System > E-Mail Notification** screen to set up an alarm to notify you when a volume is approaching full capacity.

Hot Swapping Disk Drives

The term *hot swap* refers to the ability to remove and add components to a system without the need to turn off the server or interrupt client access to files. Snap Servers permit hot swapping for disk drives. The Snap Server 14000, with dual fan and power supplies, also permits hot swapping for these components (see "Hot Swapping Fans and Power Supply Modules" on page 119).

When to Hot Swap Disk Drives

When available storage space is not at a premium, most administrators prefer to configure a RAID set with a hot spare that automatically takes the place of a failed drive. This solution assures that client access to file systems is not interrupted. In environments where configuring a hot spare is not possible, you may need to hot swap a drive.

Hot Swapping Disk Drives

You can hot swap disk drives on Snap Server RAIDs 1 or 5 by following the three basic steps outlined next:

1. **Using the Administration Tool, remove the failed drive from the RAID.**

   Navigate to the **Storage > RAID Sets** screen, and click the name of the RAID set that contains the failed drive. In the Actions column, click the failed drive's **Remove** link, and then follow the on-screen instructions. (For more details, see "Replacing Disk Drives on a RAID" on page 64.)

2. **Physically remove the failed drive from its bed, and insert the new drive.**

   The procedures for the physical removal and replacement of a disk drive for Snap Servers are explained in the next section.

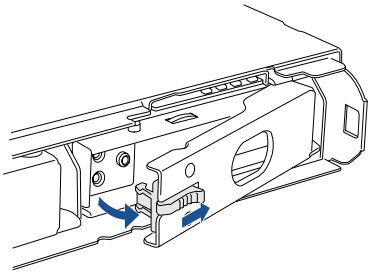
3. **Configure the new drive as part of the RAID.**

   When you remove a drive from a Snap Server, the affected RAID transitions to degraded mode. It will remain in degraded mode until the newly inserted drive is configured as a member of the RAID set via the Administration Tool. This procedure is discussed in detail on page 64.

Physically Replacing a Disk Drive on the Snap Server 4200, 4400, or 4500

When the power LED is amber and the activity LED is off, the disk drive has failed or is not working correctly.

1. Before proceeding, make sure you have logically removed the drive using the Administrator Tool as described in the previous section.
2. Remove the front bezel. With a hand on each latch, slide both latches on the front bezel toward the center. While holding the latch in the release position, pull the bezel away from the chassis.
3. On the closed handle of the failed disk drive, press the latch to the right.
4. To remove the failed disk drive, pull its handle.

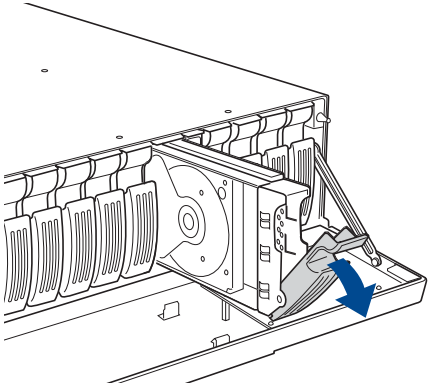


5. Release the latch on the new disk drive and open its handle. If the handle is closed, you cannot insert the disk drive completely into the bay.
6. Insert the new disk drive. Make sure that you push it forward completely before you press the handle into place.
7. Replace the front bezel.

Physically Replacing a Disk Drive on the Snap Server 14000

If a drive fails, a drive light on the front of the server flashes amber and indicates which drive has failed. The front LCD status display also indicates which drive has failed.

1. Before proceeding, make sure you have logically removed the drive using the Administrator Tool as described in the previous section.
2. Open the front panel door.
3. To pull out the failed drive, unlatch the handle and pull gently.
4. To insert the new drive, push the drive all the way forward and then push the handle until the drive is seated.
5. Close the front panel door.



Chapter 5

Security Management

The goal of security management is to control access to files in order to safeguard their integrity and confidentiality. User and group authentication along with share, directory, and file permissions are the main tools of security management, and are the focus of this chapter. The Snap Server offers local, Windows domain, and NIS domain authentication, as well as additional HTTP security options; share-level access permissions; and support for file and folder permissions.

- **Default Security Settings** — Summarizes the default settings for local authentication and share access permissions.
- **Cross-Platform Issues in Authentication** — Discusses general issues in Snap Server authentication.
- **Creating Local Users and Groups** — Provides guidelines and procedures for configuring local authentication.
- **Joining a Windows Workgroup, Domain, or Active Directory** — Provides guidelines and procedures for configuring Windows or Active Directory domain authentication.
- **Joining an NIS Domain** — Provides guidelines and procedures for configuring NIS authentication.
- **Web (HTTP, HTTPS) Authentication and Encryption** — Describes how to require users to log into the Web View screen and how to enable HTTPS encryption.
- **Setting Share Access Permissions** — Provides instructions on defining access to shares.
- **Setting File and Folder Permissions** — Explains the GuardianOS implementation of file and folder security.

Default Security Settings

Snap Server default security configuration provides one share to the entire volume. All network protocols for the share are enabled, and all users are granted read-write permission to the share.

Default Local User and Group Authentication

A *local user or group* is one defined locally on a Snap Server using the Administration Tool. The default users and groups listed below cannot be modified or deleted.

admin	The admin user account is used to log into the Administration Tool. The default password for the admin account is also *admin*.
guest	The guest user account. The default password is no password, that is, leave the password field blank.
AllLocalUsers	The AllLocalUsers group account includes all local users created on the Snap Server.
AllUsers	The AllUsers group account includes all local, Windows domain, and NIS users.
Admin	The Admin group account includes the default admin user account. Any local user accounts created with admin rights are also automatically added to this group.

Tip Windows Domain, NIS domain, and HTTP authentication, as well as HTTPS encryption are all disabled by default.

Share1 Access Protocols and Permissions

Protocol Access	The default network protocols settings and the default share settings provide access to the entire volume over all supported protocols: • Windows (SMB) • Web View (Read-only via HTTP) • NFS • AppleTalk (AFP) • FTP (Read-only anonymous user access)
Access Permissions	By default, the AllUsers group is granted read-write permission to the share.

Security Setup and Configuration Tasks

Summarized next are the steps the administrator must take to configure security on a Snap Server. Figure 1-1 summarizes the steps and methods available to the administrator to perform these tasks.

Physically Secure the Server

Place the Snap Server in a secured area with restricted access. Anyone who has access to the server could potentially reset the server or remove any hot-swappable component. The security of your data is only as good as the physical security of the server.

Disable Unneeded Network Access to the Snap Server

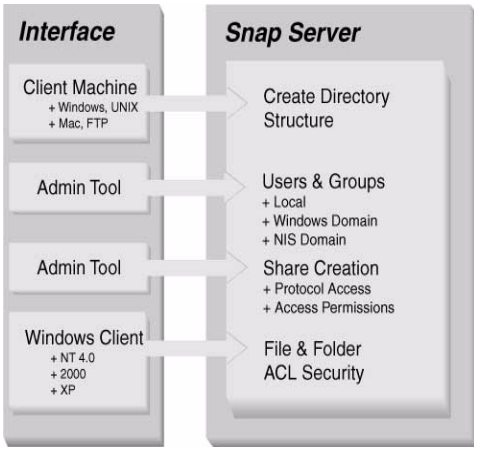
The default settings enable access to the Snap Server via all protocols supported by the Snap Server. Snap Appliance recommends that administrators disable all protocols not in use. For example, if no Macintosh or FTP clients need access to the Snap Server, disable these protocols on the Network screens of the Administration Tool.

Create the Directory Structure

The administrator has two options for creating a folder on the Snap Server. The method chosen affects how the GuardianOS assigns ownership of the directory.

- **Using a client machine —** Directories on a Snap Server created from a Windows, Macintosh, UNIX, or FTP client will have the logged-on user as the user owner of the directory, and the logged-on user's primary group as the group owner of the directory.
- **Using the Administration Tool —** When a directory is created using the **Storage > Directories** screen of the Administration Tool, the user owner of the folder will be the admin account and the group owner will be admin group.

Figure 1-1
Snap Server Security Configuration Tasks



Configure Users and Groups

Authentication validates a user's identity by requiring the user to provide a registered login name and corresponding password. Administrators have three options for configuring user and group accounts for a Snap Server.

- **Creating Local Users and Groups —** Local users and groups are created, authenticated, and maintained locally on the Snap Server.

  Tip Macintosh and FTP users must be configured as local users.

- **Joining a Windows Workgroup, Domain, or Active Directory Service —** Once joined to a Windows NT, Windows 2000 or Active Directory domain, users can authenticate to the Snap Server using their domain credentials.
- **Joining an NIS Domain —** Once joined to a NIS domain, the Snap Server can look up user and group IDs maintained by the domain.

The Snap Server also provides additional security options for authentication over the HTTP protocol using a browser:

- **HTTP Authentication —** Requires users accessing the server over HTTP to log into the server before they can view the list of shares on the Web View screen. Otherwise, users connecting over HTTP will be logged in as guest.
- **HTTPS Encryption —** *HTTPS* is HTTP using a Secure Sockets Layer (SSL). Though not itself an authentication method, HTTPS does enhance security by encrypting authentication communications between client and server.

Create Shares and Assign Access Permissions

The Administration Tool allows administrators to create a share to an existing folder, specify protocol access to the share, and set share access permissions in one wizard-like process.

Tip The GuardianOS does not support creating folders on the fly as you create a share; be sure to create the directory structure before attempting to creating shares.

Assign File/Directory Access Permissions

GuardianOS Snap Servers allow administrators to use a Windows NT 4.0, 2000, or XP workstation to assign file and directory access permissions for local and Windows domain users and groups.

Cross-Platform Issues in Authentication

Consider the issues raised in this section when choosing and implementing authentication methods in your environment.

Macintosh and FTP Access

Macintosh clients can access the server using the Guest account; FTP clients can access the server using the anonymous account. For more granular control over Macintosh and FTP access, administrators must create local user accounts for Macintosh and FTP users.

Features and Restrictions on Different Types Of Authentication

The following table summarizes the features and restrictions among local, Windows domain, and NIS domain users on the Snap Server.

	Authentication Method		
GuardianOS Feature	**Local**	**Windows Domain**	**NIS Domain**
Modify Users & Groups Locally	x		
Assign User Quotas	x	x	x
Assign Group Quotas			x
Assign File and Directory ACLs (Users and Groups)	x	x	

UIDs, GIDs, and Domain Authentication

The Snap Server is based on the Linux operating system and uses the POSIX standard system to assign user IDs (UID) and group IDs (GID). In the POSIX system, each user and group must have a unique UID. This requirement applies to all users and groups on the Snap Server, including local, NIS, and Windows users and groups. If you join the Snap Server to a Windows domain, unique IDs are automatically assigned. If you join the Snap Server to an NIS domain, be aware that the Snap Server does not recognize users or groups that are present on the NIS domain who have identification numbers outside of a specific range. The exact range is available in the online help of the Administration Tool. Navigate to the **Security > UNIX NIS** screen, click the Help button, and then click *data sheet*.

Creating Local Users and Groups

Local users or groups are created and defined locally on a Snap Server using the Administration Tool. You create local user and group accounts using the **Security > Users** and **Security > Groups** screens in the Administration Tool.

Notes on Managing Local User and Group Accounts

- **Duplicate client log-in credentials for local users and groups —** To simplify user access, duplicate client log-in credentials on the Snap Server. That is, create local accounts on the Snap Server that match those used to log into client workstations. This strategy allows users to bypass the log-in procedure when accessing the Snap Server.

  Caution This strategy applies to local users only. Do not use duplicate domain user login credentials.

- **Default local users and groups do not appear on the local users/groups screens —** The default local users and groups (page 74) cannot be modified or deleted. For this reason, they do not appear on the list of users or groups on the User or Group Management screens. The default local users and groups do appear on the Share Access and Quotas screens, however.

- **Changing UIDs or GIDs —** The Snap Server automatically assigns and manages UIDs and GIDs. Because there may be occasions when the administrator needs to assign a specific ID to a local user or group, the Snap Server makes these fields editable.

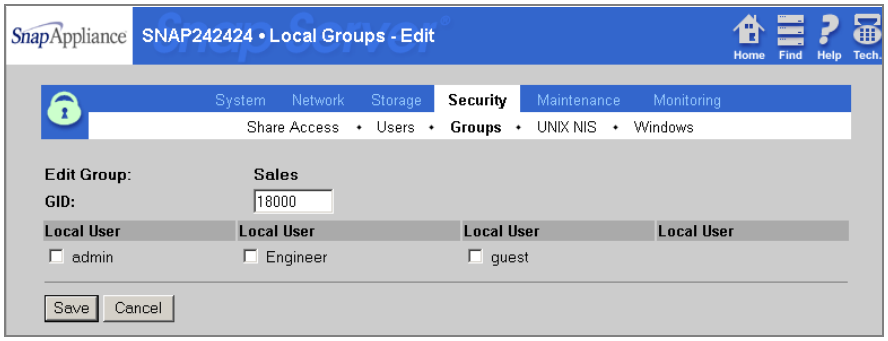
Creating Local Users and Groups

To create a local user

1. Navigate to the **Security > Users** screen.
2. Click **Create User** and enter the following information on the screen that opens:
   - A unique login name (required)
   - The user's full name (optional)
   - A unique password (required)
   - A UID (optional)
3. Click **Create**.

To create a local group

1. Navigate to the **Security > Groups** screen.
2. Click **Create Group** and enter a unique name for the group on the screen that opens.
3. To create the group, click **Create**. The Group Edit screen opens.



4. Select or Clear a user's check box to add or remove the user from the group.
5. If necessary, edit the GID.
6. Click **Save**.

Joining a Windows Workgroup, Domain, or Active Directory

Once joined to a Windows NT, Windows 2000 or Active Directory domain, the Snap Server imports, and then maintains a current list of the users and groups on the domain.

Notes on Windows Authentication

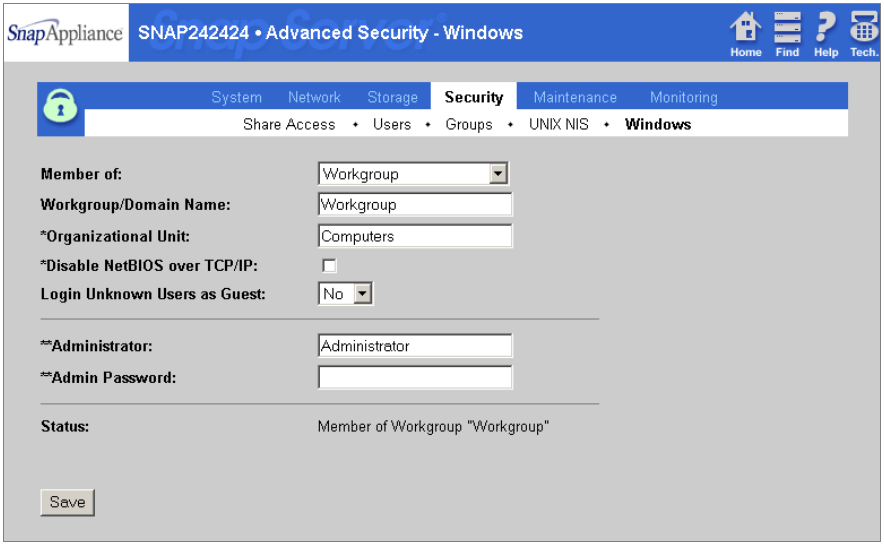
- **You cannot modify Windows domain user or group accounts locally —** You must use the domain controller to make modifications. Changes you make on the domain controller appear automatically on the Snap Server.
- **Group Quotas are not available for Windows Domain Groups —** All other Snap Server features, such as user quotas, share access, and ACLs on files and directories are available to Windows domain users and groups
- **Kerberos authentication —** The Snap Server will use Kerberos for authentication in ADS domains.
- **Support for Microsoft name resolution servers —** The Snap Server supports both of the Microsoft name resolution services: Windows Internet Naming Service and Dynamic Domain Name Server. However, when you use a dynamic domain server or a domain name server with an ADS server, make sure that the forward and reverse name lookup is correctly set up.

Interoperability with Active Directory Authentication

The Snap Server supports the Microsoft Windows 2000 family of servers that run in native Active Directory Services (ADS) mode or in mixed NT/ADS mode. Snap Servers can join Active Directory domains as member servers. References to the Snap Server's shares can be added to the LDAP database by creating a new shared folder object under an Organizational Unit.

Joining a Windows Workgroup, Domain, or Active Directory

To join a workgroup or domain, navigate to the **Security > Windows** screen. Windows or Active Directory domains resolve user authentication and group membership through the domain controller.



To Enable Guest Account Access

Select *Yes* in the **Enable Guest Account** pull-down menu to allow unknown users to access the Snap Server using the guest account. Select *No* to disable this feature.

To Join a Workgroup

1. Select **Workgroup** from the Member of pull-down menu.
2. Enter the name of the workgroup.
3. Click **Save**.

To Join a Windows Domain

1. Select **Windows Domain** from the Member of pull-down menu, and enter the name of the domain in the space provided.
2. In the administrator fields, enter a user name and password with sufficient administrative privileges to allow a remote computer to join the domain.
3. Click **Save**.

4. An error message about the use of the *restrict_anonymous* mechanism may appear along the top of the screen. If so, click the link provided on the screen to enter a valid domain (not local) user name and password that the Snap Server can use to communicate with the PDC when the Windows Authentication restrict_anonymous mechanism has been implemented on the network. For ease of administration, Snap Appliance recommends that you create a unique user account on the domain using the following guidelines: (1) Choose a name, such as *SnapServerAccess*, and include a comment that makes the function of the account clear; and, (2) Set the password to never expire.

   After you have created the unique user account and password on the domain, enter it here and click **Save**.

To Join an Active Directory Domain

1. Select **Active Directory Domain** from the Member of pull-down menu, and enter the name of the domain in the space provided.
2. You must enter the name of the organizational unit within the Active Directory tree in which the Snap Server will appear. By default, the server will appear within the container named Computers.
3. If you are using Active Directory, you may, if you wish, disable NetBIOS over TCP/IP. Select the check box to disable NetBIOS; clear the check box to leave NetBIOS enabled. If you disable NetBIOS, you must enter the domain name as a fully qualified domain name (e.g., `actdirdomname.companyname.com`). A short form (e.g., `ActDirDomName`) will not work.
4. In the administrator fields, enter a user name and password with sufficient administrative privileges to allow a remote computer to join the domain.
5. Click **Save**.
6. An error message about the use of the *restrict_anonymous* mechanism may appear along the top of the screen. If so, click the link provided on the screen to enter a valid domain (not local) user name and password that the Snap Server can use to communicate with the Domain Controller when the Windows Authentication restrict_anonymous mechanism has been implemented on the network. For ease of administration, Snap Appliance recommends that you create a unique user account on the domain using the following guidelines: (1) Choose a name, such as *SnapServerAccess*, and include a comment that makes the function of the account clear; and, (2) Set the password to never expire.

   After you have created the unique user account and password on the domain, enter it here and click **Save**.

Joining an NIS Domain

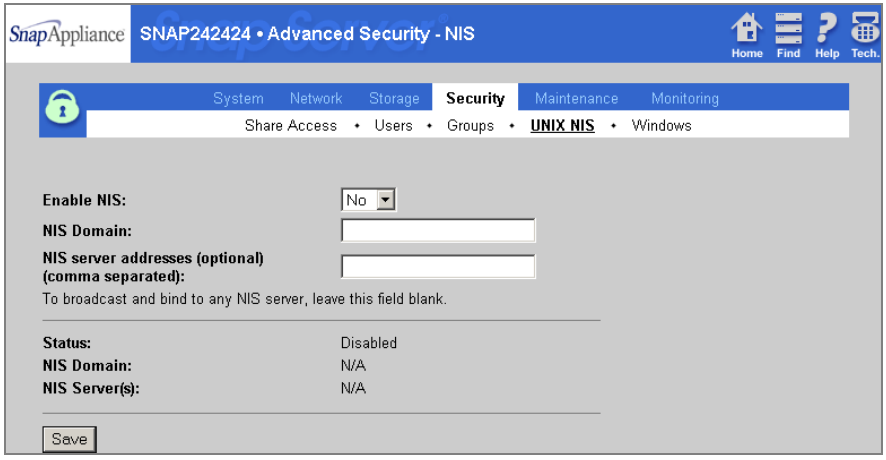
To simplify administration of multiple systems in large NFS configurations, the Snap Server can join an NIS domain and function as an NIS client. It can then read the users and groups maintained by the NIS domain.

- You cannot modify NIS user or group information locally on the server. You must use the NIS server to make modifications.
- Changes you make on the NIS server do not immediately appear on the Snap Server; it may take up to 10 minutes for changes to be replicated.
- NIS identifies users by UID, not user name, and although it is possible to have duplicate user names, Snap Appliance does not recommend this configuration.
- As a security measure, list only users who need access, rather than allowing all NFS clients access to Snap Server shares.

To join an NIS Domain

To join an NIS domain, navigate to the **Security > UNIX NIS** screen.

1 In the Enable NIS pull-down menu, select *Yes*.



2 Enter the NIS domain name.

3 To bind to an NIS server, enter one or more valid NIS server IP addresses separated by commas, or leave this field blank to bind to all available NIS server.

4 Click **Save** to join the NIS domain.

Tip To disengage from an NIS domain, select *No* in the Enable NIS field, and then click **Save**.

Web (HTTP, HTTPS) Authentication and Encryption

When a user connects to a Snap Server via the HTTP protocol, the Web View screen displays a list of all shares (and Snapshot shares, if any). Web View supports Netscape Navigator 4.7 and above and Microsoft Internet Explorer 4.0 and above. You can increase security over the HTTP protocol in two ways:

Web View Authentication

Web View authentication requires users to log in before they can view shares in Web View screen. To enable HTTP authentication, navigate to the **Network > Web** screen, select *Yes* in the Require Web View Authentication field, and click **Save**.

Secure HTTPS

HTTPS is HTTP using a Secure Sockets Layer (SSL). Though not itself an authentication method, HTTPS does enhance security by encrypting communications between client and server. To enable secure HTTPS, navigate to the **Network > Web** screen, select *Yes* in the Secure HTTP (HTTPS) field, and then click **Save**. You will be redirected to a secure HTTPS connection.

Notes on Using HTTPS

- **Browser Support —** SSL is supported by all major browsers. URLs that use SSL begin with https rather than http. This means that all browser-based transactions (using the Administration Tool, accessing the server via a browser) are available exclusively via HTTPS.
- **HTTPS and *e*Trust Inoculate*IT* —** HTTPS and the configuration of the antivirus software are incompatible. HTTPS must be disabled to access the *e*Trust Inoculate*IT* configuration interface (on the **Maintenance > Antivirus** screen).

Setting Share Access Permissions

The GuardianOS supports share-level as well as file & directory-level permissions (discussed in the next section) for all local and Windows domain users and groups.

The default permission granted to users and groups when they are granted access to the share is full control. Administrators may restrict selected users and groups to read-only access.

Share-Level Access Permissions	
Full Control	Users can read, write, modify, create or delete files and folder within the share.
Read-Only	Users can navigate the share directory structure and view files.

Notes on Share Access Behaviors

- **Share access defaults to full control —** The default permission granted to users and groups when they are granted access to the share is full control. Administrators may restrict selected users and groups to read-only access.
- **Share access permissions are cumulative —** If a user has read-only permission to the share, but is also a member of a group that has been given full-access permission to the share, the user gets full access to the share.
- **Interaction between share-level and file-level access permissions —** When both share-level and file-level permissions apply to a user action, the more restrictive of the two applies. Consider the following examples:

  Example A. More restrictive file-level access trumps share-level access.

Share Level	File Level	Result
Full Control	Read-only to FileA	Full control over all directories and files in SHARE1 *except* where a more restrictive file-level permission applies. The user has read-only access to FileA.

  Example B. More restrictive share-level access trumps file-level access

Share Level	File Level	Result
Read Only	Full Control to FileB	Read-only access to all directories and files in SHARE1 *including* where a less restrictive file-level permission applies. The user has read-only access to FileB.

Assigning Read-Only Access to NFS Users

You can assign read-write or read-only share permissions *on an individual basis* to local and Windows domain users and groups that have access to a share. That is, you can assign some users and groups read-only access to the share, and other users and groups read-write access to the same share.

The NFS protocol, however, does not support this type of user-level access control. A Snap Server share mount point will be exported, for *all* NFS clients granted access, as *either* a read-only share *or* as a read-write share. You cannot "mix" read and read-write access permissions for NFS users/groups on a single share as you can for users of other protocols such as Windows or AppleTalk.

If some NFS users need read-only access to a folder, and users accessing the server via other protocols need read-write access to the same folder, create two shares using the following guidelines:

Share to FolderA	Protocols Enabled	Share Access Permissions	Results
Share1	All Except NFS	Assign read-write or read-only access to local or Windows domain users.	Local and Windows domain users have expected access permissions.
Share2	NFS Only	Assign read-only access to all users.	Share2 exported as read-only share to NFS users.

Share1 allows "mixed" access for local and Windows users to FolderA; Share2 allows read-only access for NFS users to FolderA.

Tip Whenever you create a share (such as Share1) that assigns different access to different users and groups in the same share, *and* the NFS protocol is enabled for the share, the Administration Tool displays a warning that security settings for such shares may not apply to NFS clients. Any NFS users given access to such a share will always have read-write access.

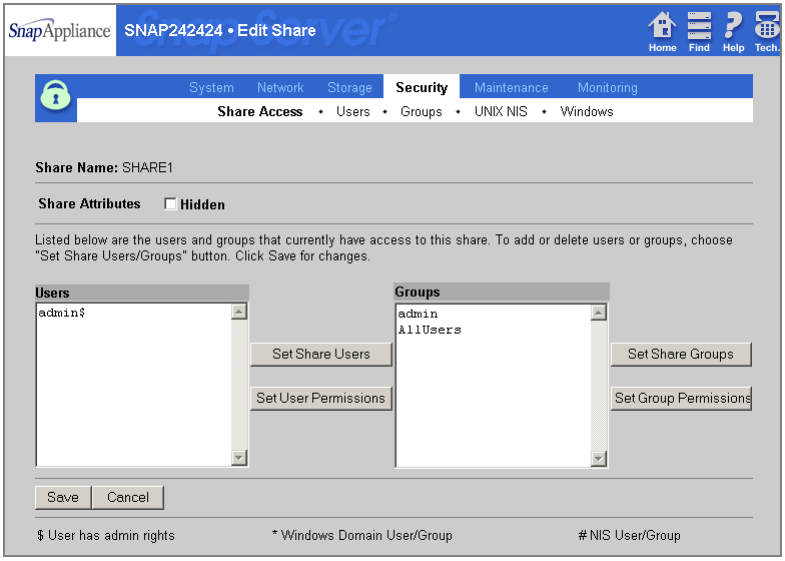
Tip To further restrict NFS access, list only users who need access (on the **Security > UNIX** screen), rather than allowing all NFS clients access to Snap Server shares.

Setting Share Access Permissions

A newly created share defaults to the following access settings:

Attribute	Default	Description
Protocol Access	All	Protocol access is set during the process of creating a share (see page 62). Unless explicitly disabled, access to the share is granted over all supported protocols.
Protocol Access Type	All	Users may view the share via any enabled protocol. The Hidden option allows an administrator to hide a share from clients connecting from the SMB, HTTP, and AFP (but not FTP or NFS) protocols.
User & Group Access Permissions	All	All users are granted access to a share by default. An administrator must explicitly grant either read-only or full control access to users and groups.

To set share access permissions, navigate to the **Security > Share Access** screen, and click the name of a share.



1 **Select or clear the Hidden check box.**

By default, the Hidden check box is cleared, and users can access the Snap Server over any enabled protocol. When the Hidden check box is selected, Windows (SMB) and AppleTalk (AFP) users will not see the share when browsing the server with either a Web browser or a file system viewer, such as Windows

Explorer. For example, assume SHARE1 is set as *hidden*. Windows users will not see the share when viewing the server through Network Neighborhood, or when performing a net view *servername* on the Snap Server.

Tip Windows users who have access rights to a hidden share can still access the share by entering the precise path to the share directly into their file system viewer. For example, Windows users could enter an address of the format \\server_name\hidden_ share_name to access a hidden share. This will not work, however, for Macintosh clients, to whom a hidden share is always inaccessible.

2 **Add (or delete) Users and Groups to the Share Access Lists.**

Adding users or groups to their respective access lists grants them full control over all files and directories in the share (subject to any file-level permissions). To add (or delete) users or groups to the share access lists, use the following procedure:

a Click the appropriate button, either **Set Share Users** or **Set Share Groups**. On the screen that opens, find the users or groups you want using one of these methods:

- **Search —** Enter a name in the field provided, and click **Search**.
- **Browse buttons —** Use the double-arrow buttons to jump to the beginning or end of the lists. Use the single-arrow buttons to browse page-by-page.

b Select users who need access to the share (or clear users who do not).

c Then click **OK** to return to the Edit Share screen. Users and groups you selected appear in their respective access list box.

d To restrict users or groups to read-only access, proceed to the next step. To grant the users and groups you have added full access to the share, click **Save**.

3 **Restrict Users and Groups to Read-Only Access as Necessary.**

To restrict users or groups to read-only access (or reset to full access), use the following procedure:

Caution NFS cannot enforce mixed share-access permissions. For more information, see page 86.

a Click the appropriate button, either **Set User Permissions** or **Set Group Permissions**.

b Select users or groups who need read-only access to the share (or clear users who do not).

c Then click **OK** to return to the Edit Share screen.

4 **Click Save.**

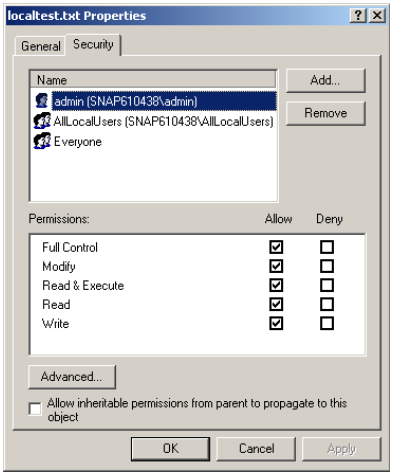
Setting File and Folder Permissions

The GuardianOS supports the use of the Windows NT, 2000, or XP interface to set directory and file permissions for local and domain/ADS users and groups on the Snap Server. On a directory, administrators can also set inheritance permissions that will be inherited by subordinate folders and files created within the directory.

Default File and Folder Permissions

When a file or directory is created, the GuardianOS grants access to the accounts listed in the following table. Access permissions for each account are inherited from the parent directory. The example displayed in the graphic shows the default settings for a file created by the local user *admin*.

File/Directory Level Access Permissions	
User Owner	Initially, the user who created the file or directory
Group Owner	The primary group of the user who created the file or directory
Everyone	Includes users to whom no other permission applies



- **The default permissions cannot be deleted —** You can delete Everyone, but the GuardianOS does not allow you to delete the user owner or group owner. You can, however, modify the permissions for these accounts as described in the next subsection.
- **Ownership is set when the file or folder is created —** The user account under which a file or folder is created becomes the owner of the file or folder. This user's primary group becomes the group owner of the file or folder.
- **The primary group of NT 4.0 or AD domain users is specified on the domain controller —** For local users, the primary group is AllLocalUsers. For Windows domain users, the primary group can be set on a Windows Domain controller. (This setting is purely for compatibility with the GuardianOS security, and is not significant in Windows security.)
- **The user owner always has change permissions permission —** Regardless of file-level access settings, a user owner has change permissions access to files and directories.

Setting File and Directory Access Permissions and Inheritance

Directory and file access permissions are set using Windows NT, 2000, or XP security tools, but not all the options available in Windows security are available on the Snap Server. The GuardianOS supports the following file and directory permissions.

File- and Level Access Permissions	
Read	Grants complete read access. It is a combination of List Folder/ Read Data, Read Attributes, Read Extended Attributes, Read Permissions.
Write	Grants complete write access. A combination of Create Files/Write Data, Create Folders/ Append Data, Write Attributes, and Write Extended attributes.
Execute	(UNIX and MacOS X only) Allows programs and scripts to run
Delete	Grants the user the permission to delete the file/directory.
Change Permissions	Grants the user rights to modify the permissions (ACLs) on the file/ directory
Take Ownership	Take Ownership gives the user the ability to take ownership of the file/ directory

You can also set inheritance for a directory such that subfolders and files created under the directory inherit a set of permissions. This inheritance should propagate to subordinate files and folders at creation time once the default behavior is set. The GuardianOS supports three levels of inheritance, as listed in the following table. The other six levels of inheritance available in Windows are not supported and will not work against a Snap Server.

Supported Inheritance Settings	
This Folder	Permissions will only be applied to the current directory and will not be inherited by subfolders or files.
Subfolders and files	Permissions will be inherited by subfolders and files, but will not be applied to the current directory.
This folder, subfolders, and files	Permissions will both be applied to the current directory and inherited by subfolders and files.

To set file and directory permissions and inheritance

1. Using a Windows NT 4.0, 2000, or XP client, map a drive to the Snap Server, logging in as a user with change permissions for the target file or directory.
2. Do one of the following:
   - In Windows NT, right-click the file or directory, choose **Properties**, click the Security button, and then click Permissions .
   - In Windows 2000, right-click the file or directory, choose **Properties**, and then click the Security tab.
3. Use the Windows security tools to add or delete users and groups, to modify their permissions, and to set inheritance rules. Be sure to keep in mind the supported features of the GuardianOS as explained in this chapter and summarized next.

How File & Directory Access Permissions are Processed

The GuardianOS processes access permissions differently than Windows. When a user attempts to perform an action on a file and directory, Windows collects all permissions that apply to the user before deciding whether to allow the user to perform the action. The GuardianOS, on the other hand, uses the first applicable permission it finds to decide whether to allow the user to perform the action. The GuardianOS searches for access permissions in the following order.

1. User Owner
2. User
3. Group Owner
4. Group
5. Everyone

When a match is found, the search stops and the specified access permission is applied. The following table shows the difference between how Windows and the GuardianOS process access permissions:

Type	Access	Windows	GuardianOS
user	Read-Only	Match found, read access found, continue searching for necessary access	Match found, stop and apply read-only permission.
group	Read-Write	Match found, grant write access	

In this case, Windows grants write access to User1 for this file, whereas the GuardianOS denies write access to User1 for this file.

GuardianOS File and Directory Access Permissions Summary

Administrators may want to keep this summary handy when setting file and directory access permissions.

GuardianOS File and Folder Access Permissions

The GuardianOS permits the following types of permissions. Bolded permissions are created by default. The user owner and group owner cannot be deleted, but their permissions can be modified by using NT 4.0, Windows 2000, XP security tools.

- **User Owner** — Usually the user who created the file
- User (non-owner) — Permission added through Windows security tools or inherited from a parent directory
- **Group Owner** — Usually the primary group of the user who created the file
- Group (non-owner) — Permission added through Windows security tools or inherited from a parent directory

Supported Permissions

The GuardianOS supports the following file and directory permissions

- **Read** A combination of List Folder/ Read Data, Read Attributes, Read Extended Attributes, Read Permissions. This gives complete read access.
- **Write** A combination of Create Files/ Write Data, Create Folders/ Append Data, Write Attributes, and Write Extended attributes. This gives complete write access.
- **Execute** (UNIX and MacOS X only) Allows programs and scripts to run.
- **Delete** Can delete the file/directory.
- **Change Permissions** Can modify the permissions on the file/directory.
- **Take Ownership** Can take ownership of the file/directory.

How Permissions are Applied

The GuardianOS searches for permissions in the order listed below; it stops and applies the first match found.

1. IF this user is the **user owner** of the file, then grant the specified access.
2. ELSE IF there is a regular (non-owner) user specified for this user, then grant the specified access.
3. ELSE IF this user is a member of the **group owner** of the file, then grant the specified access.
4. ELSE IF this user is a member of a group that is specified in a regular (non-owner) group ACE, then grant the specified access.
5. ELSE grant this user the access specified for the **Everyone** group.

Chapter 6

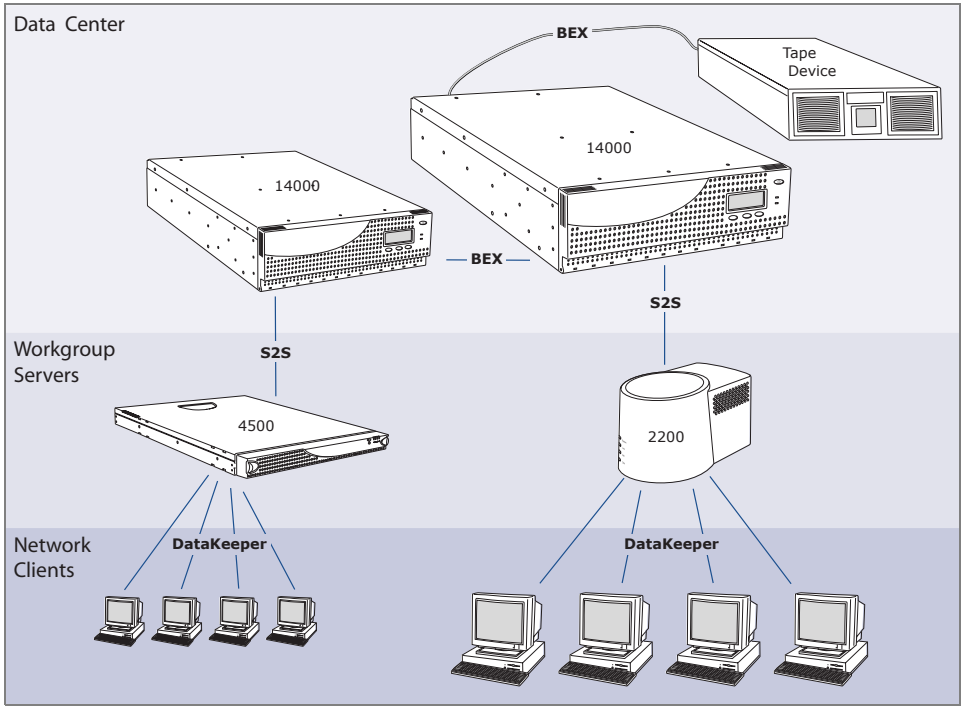
Data Protection

This chapter covers backup and disaster recovery procedures that can ensure your company's data is secured and accessible at all times. The Snap Server supports a variety of native as well as third-party technologies that you can use to implement a disaster recovery strategy appropriate to your environment and current practices. The first three sections of this chapter discuss backup options and procedures you perform before disaster strikes; the final section describes how to use these files to restore any Snap Server to its original state.

- **Data Backup Options —** Provides an overview of how you can use Snap Server Snapshot technology in conjunction with Backup Express for GuardianOS to optimize your data protection procedures. Optional third-party as well as native backup options are also discussed.
- **Using Snapshots —** Provides information you need to plan and implement Snapshots as part of your data protection strategy.
- **Using Backup Express for GuardianOS —** Provides an overview of Backup Express for GuardianOS concepts and discusses using the software to perform backup and restore operations on Snap Servers.
- **Backing Up Server and Volume Settings —** Explains how to create the files you need to recover a Snap Server's configuration information, such as network and RAID configurations, as well as volume-specific information, such as ACLs and quota settings.
- **Disaster Recovery Procedures —** Discusses what to do if all access to the data on a Snap Server is cut off due to a hardware or software failure. Focus is placed on the procedures for: (1) reinstalling the Snap Server operating system; and, (2) restoring the server to its original configuration with data intact.

Data Backup Options

Snap Appliance provides four native applications—Snapshots, Backup Express for GuardianOS, Server-to-Server Synchronization, and DataKeeper —that you can use to enhance your backup procedures. Backup Express for GuardianOS provides native tape backup support, Snapshots ensure that the file system you back up is internally consistent and complete, and S2S provides an alternative way to back up data to disk. If you wish, you can also use backup products from Computer Associates, Legato, and Veritas with your Snap Server.



Using Snapshots to Optimize Data Backup

Snapshots can satisfy minor, short-term backup situations such as recovering a file deleted in error, or even restoring an entire file system, without resorting to tape. More importantly, Snapshots can be incorporated as a central component of your backup strategy to ensure that all data in every backup operation is internally consistent and that no data is overlooked or skipped.

- **On-demand file recovery —** A Snapshot share (see page 100) provides users with direct access to archived versions of their files. Users who wish to view or recover an earlier version of a file can retrieve it on-demand without administrator intervention.

- **Snapshot rollback —** If you need to restore a file system to a previous state, you can do so without resorting to tape. The rollback feature allows you to use any Snapshot to restore an entire volume to a previous state, including ACL and quota information.
- **Backup optimization —** When you back up a live volume directly, there is a chance that the internal consistency of the file system may be compromised; that is, files that reference other files in the system may become asynchronous. The more data you have to back up, the more time is required for the backup operation, and the more likely these events are to occur. By backing up the Snapshot rather than the volume itself, you greatly reduce the risk of archiving inconsistent data.

Backup Express for GuardianOS

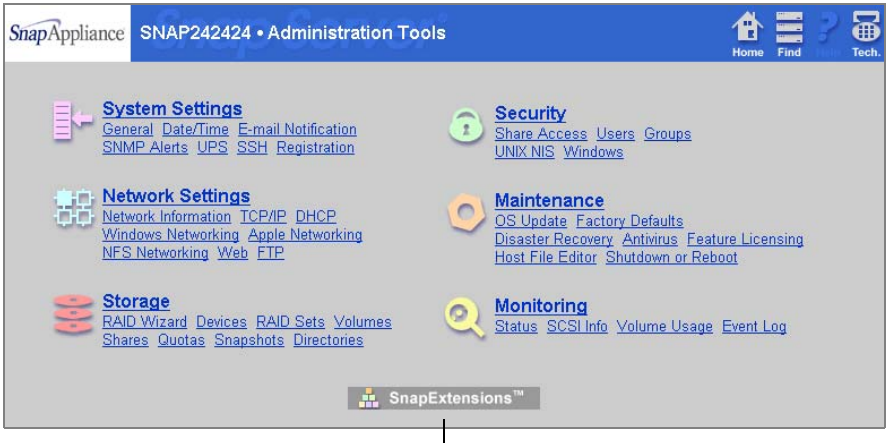
Backup Express for GuardianOS is a comprehensive backup solution from Syncsort Inc. The master server component of the Backup Express software is preinstalled on your server to support backup and restore operations to a local tape drive. The default installation supports the following features:

- **Local Backup —** The default configuration supports local backup operation where data is streamed from the Snap Server directly to a locally attached tape device. In multi-server installations, data from up to four additional source Snap Servers can be streamed over the IP network to a tape device connected to a destination Snap Server.
- **Tape Drive Support and Management —** Backup Express for GuardianOS is compatible with all tape formats including DLT, LTO, and AIT. A single central database (known as the catalog) tracks all files and the tapes on which they reside. Backup Express offers advanced scheduling capabilities that enable you to run backups without any administrator intervention.
- **Disaster Recovery Support —** Complete backup and restore of all extended Extended POSIX ACLs of the Snap Server is supported.
- **Upgrading to Jukebox Support —** Robotic tape library support enables unattended, lights-out backup operations (upgrade required, see “Upgrading Backup Express for Jukebox Support” on page 163 for more information).

The Snap Server ships with the Backup Express for GuardianOS CDs. These CDs contain client applications (GUI) as well as a Getting Started Guide that walks you through the initial configuration tasks and introduces you to the Backup Express GUI. Use the installation CDs to install the Backup Express GUI software on a Windows or UNIX workstation.

Server-to-Server Synchronization

Server-to-Server Synchronization (S2S) is a SnapExtension that copies the contents of a share from one Snap Server to another share on one or more different Snap Servers. Any Snap Server server can be used as either a source or a destination for replicated content. Once you set up a synchronization task, the source server sends messages advising all destination servers to begin synchronizing data. The files on the source server are compared with the same files on the destination server. Files that have been modified are replicated to the destination server, overwriting the previous copy.



SnapExtensions button

S2S works with all Snap Server models. The S2S software is preinstalled on all GuardianOS Snap Servers. (The S2S software is available for download from the Snap Appliance Web site for SnapOS Snap Servers.) To access the S2S configuration screens, connect to the browser-based Administration Tool and click the **SnapExtensions** button. Detailed configuration procedures for S2S are available in the online help.

PowerQuest DataKeeper

PowerQuest DataKeeper allows you to configure user workstations or laptops to automatically back up data to a Snap Server. Users do not need to remember to copy important data to the server for regular backup; Datakeeper does it for them in the background. DataKeeper can be configured to back up user data each time their PC starts, and to continuously monitor all data and system files that are changed during the session. The DataKeeper software is included with every Snap Server. For more information in installing and configuring DataKeeper, see the DataKeeper Quick Start Guide provided with your Snap Server.

Supported Native and Third-Party Backup Solutions

The GuardianOS Snap Server supports the following native and third-party backup solutions.

Snap Server Backup Solutions		Native Backup Solutions			Third-Party Backup Solutions										
					Windows					UNIX/Linux					Mac
		Backup Express for GuardianOS	Server-to-Server Synchronization	DataKeeper 5.0 (Windows)	CA BrightStor ARCserve 2000 v7	CA BrightStor Enterprise Backup v10	Legato NetWorker 6.1.1	Veritas Backup Exec v 8.6	Veritas NetBackup DataCenter 3.4.1	CA BrightStor ARCserve v7	CA BrightStor Enterprise Backup v10	Legato NetWorker 6.1.1	Veritas Backup Exec v 8.6	Veritas NetBackup DataCenter 3.4.1	Dantz Retrospect Express Server 5.0
GuardianOS 2.4	Snap Server to Backup Server via installed agent	x			x	x	x	x	x	x	x	x	x	x	
	Snap Server to Backup Server via network protocol	x			x	x	x	x	x						x
	Snap Server to Snap Server		x					x							
	Snap Server(s) to SCSI-attached tape drive	x													
	Client to Snap Server			x											
	Backs Up ACL Security Data	x													

Configuring third-party backup solutions

To configure a Snap Server to work with one of the supported backup solutions, you must: (1) install the backup agent software on the Snap Server; (2) inform the Snap Server of the IP addresses of each backup master server; and, (3) inform the backup software of the Snap Server's IP address. Instructions for these procedures are given in "Third-Party Backup Applications" on page 153.

Tip On a Macintosh computer, you must mount the appropriate shares (volumes) on the desktop so that the Macintosh backup programs can operate without a remote agent.

Using Snapshots

A *Snapshot* is a consistent, stable, point-in-time image of a volume used for backup purposes. For the life (duration) of the Snapshot, before new data is written to the live file system, the original data is written to the Snapshot, thus preserving the original image. Snapshots consume a minimum of storage space because they record only data that has changed.

How Snapshots Impact Performance

When a Snapshot is active, you may experience a slight drop in write performance on new writes to the file system because the original data must be written to the most recent Snapshot before any new data is written to the live file system. Depending on the situation, the drop in write performance may range from five to ten percent.

Snapshot Chaining

Chaining technology resolves both the storage cost and performance issues formerly associated with Snapshots. Because each Snapshot 're-uses' data from more recent Snapshots, no space is wasted, and only one write to disk (for the most recent Snapshot) is required to maintain all the Snapshots, regardless of how many exist.

This dependency of newer Snapshots on all previous Snapshots means that when you delete a Snapshot, all previously taken Snapshots are also deleted. Also, any expired snapshots will not be deleted until the snapshot that has a dependence upon it has expired, or is deleted. For example, if ten Snapshots currently exist (with number ten being the most recent), and you delete Snapshot number five, Snapshots one through four will lose the source of some of their data, rendering them invalid, and thus the Snap Server deletes them as well.

Recurring Snapshots

A recurring Snapshot runs according to a schedule you specify. A recurring Snapshot schedule works like a log file rotation, where a certain number of recent Snapshots are automatically generated and retained as long as possible, after which the oldest Snapshot is discarded.

Managing the Snapshot Pool

Snapshots are stored on a RAID in a *Snapshot pool*, or space reserved within the RAID for this purpose. Each RAID may contain only one Snapshot pool, which contains all Snapshots of all volumes on the RAID.

Snapshots grow dynamically for as long as they are active and as long as there is enough space available in the Snapshot pool to store them. When the Snapshot pool approaches its capacity (at about 95%), the Snap Server deletes the oldest Snapshot to create space for more recent Snapshots.

The default configuration allots 80% of RAID capacity to the volume and 20% to the Snapshot pool. You can adjust the size of the pool up or down according to your needs. If Autodeletion removes older Snapshots more frequently than your backup strategy allows, consider increasing Snapshot pool capacity.

The number of Snapshots that the Snap Server can support is a function of: (1) the space reserved for the Snapshots; (2) the duration of the Snapshots you create; and, (3) the amount and type of write activity to the volume(s) since the Snapshot was created. The following table describes minimum and maximum allocation cases.

Allocate about 5% of RAID if	Allocate about 25% of RAID if
• Activity is write-light	• Activity is write-heavy
• Write access patterns are concentrated in a few places	• Write access patterns are randomized across the volume
• Snapshots need not remain available for long periods	• Snapshots must remain available for long periods

To Adjust Snapshot Pool Capacity

1. Navigate to the **Storage > Snapshots** screen, and click the **adjust snapshot space** link in the introductory text.
2. In the screen that opens, type a new number for the volume for which you want to increase or decrease Snapshot space.
3. Click **Save.**

Accessing Snapshots

Snapshots are accessed via a Snapshot share. Just as a share provides access to a portion of a live volume (or file system), a Snapshot share provides access to the same portion of the file system on all current Snapshots of the volume. The Snapshot share's path into Snapshots mimics the original share's path into the live volume.

You create a Snapshot share by selecting the **Create Snapshot Share** option in the course of creating a live-volume share. For example, assume you create a share to a directory called "sales," and you select the **Create Snapshot Share** option, Web View will display two shares as follows:

```
SALES
SALES_SNAP
```

The first share provides access to the live volume, and the second share provides access to any archived Snapshots. Other than read/write settings (Snapshots are read-only), a Snapshot share inherits access privileges from its associated live-volume share.

A Snapshot share contains a series of directories. Each directory inside the Snapshot share represents a different Snapshot. The directory names reflect the date and time the Snapshot was created. For example, assume the Snapshot share named `Sales_SNAP` contains the following four directories:

```
latest 2002-12-25.120000 2003-01-01.000100 2003-01-07.020100
```

The `latest` directory always points to the most recent Snapshot (in this case, `2003-01-07.020100`, or January 7th, 2003, at 2:01 a.m.). A user may view an individual file as it existed at a previous point in time or even roll back to a previous version of the file by creating a file copy to the current live volume.

Tip You can create (or remove) a Snapshot share at any time from the Share > Edit screen. Navigate to the **Storage > Shares** screen and click a share name. In the screen that opens, simply click the **Create Snapshot Share** (or Delete Snapshot Share) check box, and then click **Save**.

Creating and Scheduling Snapshots

To create a Snapshot, navigate to the **Storage > Snapshots** screen. Creating a Snapshot involves first defining the Snapshot and then scheduling the Snapshot. For regular data backup purposes, create a recurring Snapshot that runs at an administrator-configured time and interval. You can also create individual, one-time-only Snapshots as necessary.

Tip If you have created a new volume or have numerous existing Snapshots, make sure you have enough space allocated in the Snapshot pool as described on page 99; otherwise, you will not be able to create the Snapshot.

1 **Create the Snapshot definition.**

To begin the process, click **Create Snapshot**. In the screen that opens, complete the following information to define the Snapshot:

- Name the Snapshot.
- Identify the source volume.
- If you plan to create a tape backup from the Snapshot, choose *Yes* from the Create Recovery File pull-down menu. (See the next section for information on coordinating Snapshots and backup operations.)

Click **Continue** to schedule the Snapshot.

2 **Run the Snapshot now or schedule it to run later.**

Specify the start time as **Now** (the default) and proceed to the next step, or choose **Later** and complete the following fields:

- Schedule a date and time to run the Snapshot.
- To repeat a Snapshot periodically, select **Recurring** and specify the Repeat Interval in hours, days, weeks, or months.

3 **Specify the duration of the Snapshot.**

In the Duration field, specify how long the Snapshot is to be active in hours, days, weeks, or months. The Snap Server automatically deletes the Snapshot after this period expires, as long as there are no older unexpired Snapshots that are dependent on it. If any such Snapshots exists, its termination date is displayed at the bottom of the screen. You must set the duration to a date and time after the displayed date.

4 **Create the Snapshot.**

Click **Create**. If you elected to run the Snapshot immediately, it appears in the Current Snapshots table. If you scheduled the Snapshot to run at a later time, it appears in the Scheduled Snapshots table.

Coordinating Snapshot and Backup Operations

Like backups, Snapshots can be scheduled to recur at a designated time and interval. In addition to synchronizing the backup and Snapshot schedules, you must create a share (and Snapshot share) to the root of the volume so that the backup software can access the Snapshot.

1. **Create a Snapshot for each volume you want to back up.**

   In the Administration Tool, navigate to the **Storage > Snapshots** screen, and click **Create Snapshot**. When defining and scheduling the Snapshot, consider the following:

   - In the Create Recovery File pull-down menu, select *Yes* to ensure that the ACL and quota information current at the time the Snapshot is captured is appended to the Snapshot. This step is needed because many backup packages do not backup native ACLs and quotas. Placing this information in a recovery file allows all backup systems to include this information. If the volume needs to be restored from tape, or the entire system needs to be recreated from scratch on a different server, this information may be required to restore all rights and quota information.
   - Offset the Snapshot and backup schedules such that the backup does not occur until you are sure that the Snapshot has been created. (The Snapshot itself does not require much time, but creating the recovery file may take up to 30 minutes, depending on the number of files in the volume.) For example, assuming you schedule nightly backups for a heavily used volume at 3 a.m., you might schedule the Snapshot of the volume to run every day at 2:30 a.m., allowing half an hour for the Snapshot to run to completion.

2. **Create a share for each volume with Snapshot Share enabled.**

   In the Administration Tool, begin by clicking the **Security > Shares** screen, and click **Create Share**. Select the volume and click **Continue**. Then, to create a share to the volume itself (on the root), simply accept the default path by clicking **Use Current Path**. Finally, be sure to select **Create Snapshot Share**.

3. **Set the backup software to archive the latest version of the Snapshot.**

   The Snap Server makes it easy to configure your backup software to automatically archive the most recent Snapshot. Simply configure your backup software to copy the contents of the `latest` directory within the Snapshot share you created at the root of the volume. For example, assume the Snapshot share named `SHARE1_SNAP` contains the following four directories:

   ```
   latest 2002-12-25.120000 2003-01-01.000100 2003-01-07.020100
   ```

Each directory inside the Snapshot share represents a different Snapshot. The directory names reflect the date and time the Snapshot was created. However, the `latest` directory always points to the latest Snapshot (in this case, `2003-01-07.020100`, or January 7th, 2003, at 2:01 a.m.). In this case, configuring the backup software to copy from

```
\SHARE1_SNAP\latest
```

ensures that the most recently created Snapshot is always archived.

Snapshot Rollback

If you need to restore a file system to a previous state, you can do so without resorting to tape. The Snapshot rollback feature allows you to use any archived Snapshot to restore an entire file system to a previous state simply by selecting the Snapshot and clicking the Rollback button. During the rollback operation, data on the volume will be inaccessible to clients.

Tip Performing a rollback on a volume may invalidate the Backup Express for GuardianOS catalog for the volume. For this reason, it is important to synchronize catalog backup operations with your Snapshot schedule. A rollback operation may also disable the antivirus software. If you are using these features, take the necessary precautions as described on page 58.

1. Navigate to the **Storage > Snapshots** screen, and click the name of the Snapshot you want to use for the rollback operation.
2. Click **Rollback**. One the confirmation screen that opens, click **Continue**.

   The time required to complete the rollback operation depends on the amount of changes to be rolled back. You can track the progress of the operation from **Storage > Volumes** screen.

Using Backup Express for GuardianOS

This section provides an overview of Backup Express for GuardianOS concepts and discusses using the software to perform backup and restore operations on Snap Servers. The procedures for installing the Backup Express GUI on a client machine and performing basic configuration tasks are described in the Quick Start Guide, found in the sleeve of the Backup Express for GuardianOS User CD. The presentation of this content assumes that you have performed these procedures.

The extensive documentation set provided on the Backup Express for GuardianOS CD covers the full Backup Express product, including modules not supported by the default Snap Server installation. Information presented here is specific to the GuardianOS and has been adapted primarily from two sources: Backup Express Operations Guide (bexoper.pdf) and the Configuration Guide (bexconf.pdf). For more information on the procedures described in this section, see the appropriate document.

Supported Configurations

The default installation supports either a highly distributed configuration, where a storage device is attached to each Snap Server on your network; or a centralized configuration, where a tape device is attached to one Snap Server (acting as the master server) and up to four "satellite" Snap Servers as nodes. Highly distributed processing (single storage devices on numerous nodes) gives you the greatest speed, since you have many device servers processing concurrently. There is a cost, however, in tape management. At the other end of the spectrum, using centralized media pools provides greater administrative convenience in exchange for reduced processing speeds.

Tip To maximize performance, the GuardianOS eliminated all system control and processing functions, including e-mail, that do not contribute to improving file I/O throughput. For this reason, the e-mail reporting functions of Backup Express will not work on Snap Servers.

Components

Backup Express for GuardianOS is comprised of the following major components.

- **Snap Server Master Server —** A *master server* is one that contains the Backup Express product, including the catalog and modules that control media management, scheduling and distributed processing. This software is preinstalled on all Snap Servers.
- **Backup Express GUI —** The Backup Express graphical user interface (GUI) is used for all configuration and administrative tasks. For information on installing, launching, and using the Backup Express GUI for configuration tasks, see the Backup Express for GuardianOS Quick Start Guide in the sleeve of the User CD.
- **The Catalog —** The *catalog* is a file stored on the Snap Server that keeps track of the data you back up. The catalog records the data's original location on the network, the data's current location on a media volume, and the date and time the backup was performed. Restore operations will fail if this file is deleted.

Backup Modes

A *backup mode* is a method of backing up data devised for a particular type of data. Backup Express for GuardianOS offers three backup modes:

- **File —** Use file mode to logically back up data by file and directories. File mode is what you normally think of when you think of backups. You will work in this mode for most of your backups.
- **Catalog —** Use catalog mode to back up the Backup Express for GuardianOS catalog. Preserving a recent copy of your catalog is essential to restoring data, particularly in disaster recovery situations.
- **Raw —** Use raw mode to performs a physical backup in which Backup Express for GuardianOS reads the disk block by block and writes it exactly as it reads it. This is used primarily to back up database files that are written in the raw format.

Restore Modes

A *restore mode* is a method of restoring data appropriate to particular situations or types of data. Backup Express for GuardianOS offers four restore modes:

- **Catalog —** Use catalog mode to specify exactly what to restore. In catalog mode, Backup Express displays your enterprise tree structure. You can select data to restore at the node group, node, drive, directory, or file level.
- **Definition —** Use definition mode to restore all the data in a specific backup definition. Backup Express displays all the backups you have defined and the dates on which they were performed. You can choose a backup from a specific date and a backup scheme, such as the last differential backup for the selected backup definition. This approach is expedient if you want to restore large amounts of data.
- **Tape —** Use tape mode to restore data from an uncataloged Backup Express tape. Backup Express brings up a dialog box that allows you to specify a search pattern. Backup Express restores the files that match your parameters.
- **Raw —** Use raw mode to restore data backed up in raw mode. This mode displays a list of the raw partition backups. Simply select the backup to restore.

Planning Backup Procedures

The goal of any backup strategy is to design a backup schedule that utilizes your resources efficiently and provides the data protection you need. You can create multiple backup definitions and have a different intention for each. When determining your backup requirements, consider the following:

- The amount of data on your system
- The frequency with which it changes
- How many versions you want to save
- How long you want to retain tapes
- How many tapes you want to manage
- File system activity at the time of backup (If heavy, consider backing up a Snapshot rather than the live file system)

Start your plan by analyzing what you want to save and, beyond that, how you will want to restore it. Does your backup definition cover your entire enterprise or just a department or project? Is your goal to be able to restore your entire system as quickly and easily as possible in the event of a disaster? Or do you want to restore the occasional lost file or node? When you devise a backup schedule, you are weaving a safety net for your data out of the three types of backups known as backup schemes.

Backup Schemes

A backup schedule incorporates one of the following three types of operations known as backup schemes:

- **Base —** Backs up all target files on the Snap Server
- **Differential —** Backs up all target files on the Snap Server that have changed since the last base backup of the same name
- **Incremental —** Backs up target files on the Snap Server that have changed since the last backup of any type with the same name

Each backup scheme may have different parameters such as a different schedule or a different output destination. However, the schemes must share the same input source. Therefore, a backup definition includes all three backup schemes as well as all the parameters governing them. Since they are part of the same backup definition, they are referred to by the same name.

Sample Backup Schedules

The following three sample backup schedules illustrate how the three backup types interact.

Network A has a base backup scheduled for every Sunday and an incremental backup scheduled for all the other days of the week. All the backups are performed at 2:00 am. If on Sunday at 1:00 am, all the data on the network is lost, it would take 7 tapes, 1 base plus 6 incrementals, to restore the entire enterprise.

Network B has a base backup scheduled for every Sunday and a differential backup scheduled for every other day of the week. All the backups are performed at 2:00 am. If on Sunday at 1:00 am, all the data on the network is lost, it would take 2 tapes, 1 base plus 1 differential, to restore the entire enterprise.

Network C has a base backup scheduled for every Sunday, a differential backup scheduled for every Thursday, and an incremental backup scheduled for every other day of the week. All the backups are performed at 2:00 am. If on Sunday at 1:00 am, all the data on the network is lost, it would take 4 tapes, 1 base, 1 differential, and 2 incrementals, to restore the entire enterprise. Remember, the differential backup copies all the data that has changed since the last base backup. Therefore, the Thursday differential backup backs up all the data that was changed on Monday, Tuesday, and Wednesday in addition to any data that changed on Thursday.

Backing Up Data

Backing up data involves creating a backup definition and then scheduling the backup. A *backup definition* is a set of parameters that define key elements of a backup operation. To access the Backup Definition screen, click **Backup** at the Administrator Menu. The Backup Definition screen opens.

1 **Name the backup definition.**

Click the **New Backup Definition** button. In the Define New Backup Job dialog box that opens, enter a unique job name and click **OK**. The name appears in the title bar of the screen.

2 **Identify data to back up.**

In the Backup Mode pull-down menu, make sure *Files* is selected. The source window on the left displays a tree structure of any Snap Servers you have defined to the software. Double-click icons to navigate to the directory you want to back up, then select the directory. (In the default Snap Server configuration, select SHARE1).

Tip To select or deselect directories, click the yellow icon next to the node group, node, disk, directory, or file icon. A red-filled icon indicates a selected item.

3 **Identify the destination for the backup.**

A default destination is configured by the administrator when nodes groups are defined. If you accept the default location, you do not have to explicitly assign a destination. To assign a destination other than the default, use the following procedure:

a In the Source Nodes window on the left side of the screen, click the name of the node group or node you want to specify a destination for.

b Double-click on any of the icons in the Destinations For window on the right side of the screen to open the Destination Settings Window.

c Select the device cluster (or jukebox) and the media pool you want to use, and then click **OK**.

4 **Run the backup or Schedule it to run at a future time.**

- To run the backup immediately, click the **Go** button. You will be prompted to save the backup definition. Click **Yes**, and the backup operation begins.
- To schedule the backup operation, click the Stopwatch button along the top of the screen. For instructions on using the Scheduler dialog box that opens, see page 111. When finished, save the backup definition.

Restoring Data

Restoring data involves creating a restore definition and then scheduling the restore. A *restore definition* is a set of parameters that define key elements of a restore operation. To access the Restore Definition screen, click **Restore** at the Administrator Menu. The Restore Definition screen appears.

1 **Name the restore definition.**

Click the **New Restore Definition** button. In the Define New Restore Job dialog box that opens, enter a unique job name and click **OK**. The name appears in the title bar of the screen.

2 **Specify the data to restore.**

In the Restore From pull-down menu, make sure *Definition* is selected. The source window displays all the existing backup definitions.

3 **Double-click on the definition you wish to restore.**

A list of all the base, incremental, and differential backups that have been done for that definition appears. Select a backup from the list and click on it.

4 **Specify the device cluster (or jukebox) from which to restore.**

Backup Express for GuardianOS automatically backs up to the original location. When you run the restore, you will be prompted to mount the backup media into the device cluster recorded in the Backup Express catalog as the original cluster. (If the tape is contained in a tape library which is also the original location, Backup Express for GuardianOS will mount the tape automatically.)

To specify a different device cluster, click **<Original Location>**. In the Specify Restore Devices dialog box that opens, do one of the following:

- To use a device cluster or jukebox, click the box next to its icon.
- To use a specific device, click the blue arrow to display devices in a cluster or jukebox, then select the device by clicking the box next to its icon.

5 **Specify the Snap Server to which you are restoring data.**

- To restore data to its original location, click the yellow button next to <Original Location>. You are finished with this procedure.
- To restore to a new location, click on the yellow button next to New Location. In the Specify Restore Destination dialog box that opens, click the blue arrow to expand the tree, and select a disk or directory. (Make sure the disk has enough room to hold the backed up data.)

6 **Run the restore or Schedule it to run at a future time.**

- To run the restore immediately, click the **Go** button. You will be prompted to save the restore definition. Click **Yes**, and the restore operation begins.

- To schedule the restore operation, click the Stopwatch button along the top of the screen. For instructions on using the Scheduler dialog box that opens, see page 111. When finished, save the restore definition.

7 **Save the restore definition.**

Click **Save**.

Source and Destination Options

Backup definitions come with a comprehensive set of defaults source and destination settings, such as tape-handling and data verification techniques, that simplify the definition creation process. These settings control how Backup Express for GuardianOS behaves during a backup or restore operation when it encounters certain situations involving files and nodes. The defaults are preset to optimize performance in most environments; you should not need to alter them. If you should find you need to change one of the default settings, you can do so from the Job Defaults menu.

To view or change default settings

On the Configuration Menu, click the **Defaults** button. On the Job Defaults menu that opens, click on one of the four buttons to display a dialog box in which you can set default options. Thereafter, the new settings are applied automatically to any new backup or restore definition you create.

Tip Do not enable software compression. To do so will negatively impact performance.

Scheduling Backup and Restore Operations

Both backup and restore operations can be scheduled to run immediately or periodically. When defining a backup operation, you can use either a preset schedule or a custom schedule; when defining a restore operation, you must use a custom schedule.

To schedule a backup or restore operation, click the Stopwatch button along the top of the Backup Definition or the Restore Definition screen. The Scheduler dialog box opens.

To use a preset backup schedule (backup only)

The two pre-set backup schedules are Base/Incremental and Base/Differential. They are weekly schedules that run a base backup once a week and an Incremental or Differential backup on the remaining days.

1. Choose the Backup Schemes option, then select one of the following options:
   - *Base Incremental* schedules one base backup per week and an incremental backup on the remaining days
   - *Base Differential* schedules one base backup per week and a differential backup on the remaining days
2. Use the pull-down menus to set the day and time the base backup is performed, how often the incremental or differential backup is performed, and dates, such as holidays on which to skip the backup.

To create a custom schedule

The preset backup schedules only allow you to back up on a weekly basis. The custom schedule lets you back up on a daily, weekly, or monthly basis.

1. Choose the Custom Schedule option.
2. Choose how often you want the backup to occur by clicking the **Monthly**, **Weekly**, or **Daily Tool** button on the top right corner of the screen.
3. Specify the time of day when you want the backup to run in the Sched Time field.
4. Choose the backup scheme by clicking on one of the Backup Type buttons. Typically, you define the base backup first.
5. Use the calendar portion of the screen to indicate the days when you want a backup to run. For example, if you are using the Weekly Tool, clicking on any Friday schedules a backup for every Friday. If you are using the Monthly Tool, clicking on the first of any month, schedules a backup for the first of every month. Since the backup schemes are color coded, the day changes to the color associated with the backup scheme. For example, if you are scheduling a base backup for Friday the 3rd, Friday the 3rd changes to green when you click it.
6. Select either *Skip Run* or *Keep Schedule* in the When Holiday field to skip or run a backup operation that falls on a holiday.
7. Click **OK**.

Managing the Catalog

Because the catalog tells you which tape contains the most recent version of a file, it is vital that you back up the catalog regularly. Restoring your system in the event of a severe system failure will be arduous and time-consuming without a usable copy of the catalog. Without the catalog, you will have to rely on manual tracking of backups.

Tip The Snap Server is preconfigured with a single volume. The catalog resides in a hidden portion of this volume. If you delete this volume, the catalog information will be lost. In addition to regular catalog backups, be sure to backup the catalog before reconfiguring a Snap Server.

To back up the catalog

1. **Prepare the backup media.**

   Manually load the tape on which the catalog is stored to the appropriate device.

2. In the Backup Express GUI, navigate to the Backup Definition screen.

   On the Administrator Menu, click Backup.

3. **Select catalog from the Backup Mode pull-down menu.**

   You do not need to specify input for the backup. Backup Express knows the name and location of its catalog.

4. **Select a destination for the catalog backup.**

   In the Source Nodes window, click **<Backup Catalog>** to populate the Destination window with media icons. Double-click any of these icons to open the Destination Settings dialog box and select the device cluster and media pool to use.

5. **Save the restore backup definition.**

   Click the **Save** button. When prompted, enter a name for the definition.

6. **Schedule or run the catalog backup.**

   To run the backup immediately, click the **Go** button. To schedule the backup to run at a later time, click the **Stopwatch** button.

7. **Record the volser and partition number of the catalog backup.**

   This information is required to restore a catalog. Once the job is run, you can get this information by navigating to the Administrator Menu and clicking the **Jobs** button. On the Job Monitor screen that opens, double-click the name of the catalog backup job.

To restore the catalog

Make sure you know the volser number and the partition number (on the tape drive on which the catalog is stored).

1. **Prepare the backup media.**

   Manually load the tape on which the catalog is stored to the appropriate device.

2. **Open the Define Catalog Restore dialog box.**

   From the Administrator Menu, select the **Catalog** button. On the Catalog Menu that opens, click the **Catalog Restore** button to open the Define Catalog Restore dialog box.

3. **Complete the following fields** (leave other fields at their default settings)**:**

   - Enter either the IP address or the host name of the Snap Server to which you are restoring the catalog in the Server IP/Host Name field.
   - Select *Unix* In the Server Type field.
   - Enter either the IP address or the host name of the Snap Server to which the tape drive is attached in the Device Server IP/Host Name field.
   - Enter the path to the device file (e.g., /dev/nst0) in the Physical Device Filename field.
   - Select the media type used in the drive (e.g., DLT) in the Physical Device Type field.
   - To enter a volser in the Volser table, click **Add** to open the Specify Restore Volume Information dialog box. Enter the appropriate information and click **OK**.

4. Click **OK**.

Condensing the Catalog

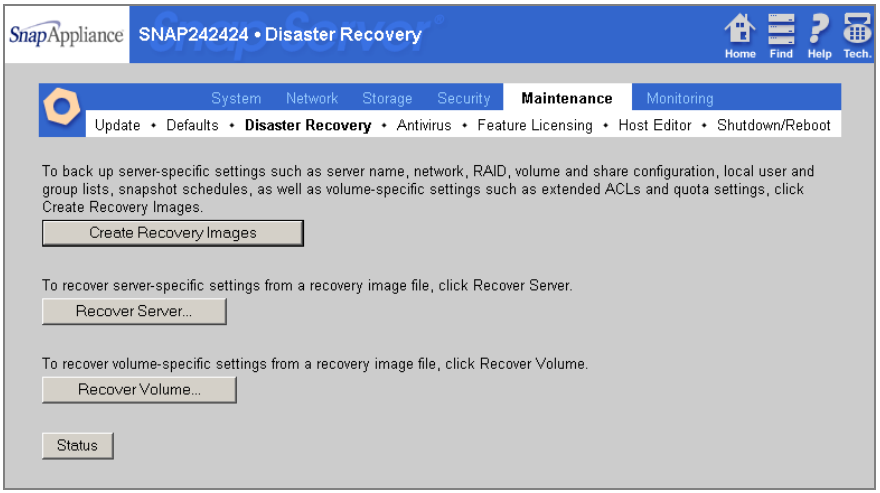
The condense operation identifies and removes expired media volumes (those that have exceeded their retention period), thus reducing the size of the catalog and allowing Backup Express for GuardianOS to run more efficiently. Condense is the primary catalog maintenance operation and it should be performed on a regular basis. As with other Backup Express for GuardianOS functions, you can run a condense operation immediately or on a schedule.

1. From the Administrator Menu, click the **Catalog** button.
2. On the Catalog Menu, click **Catalog Condense**. The Catalog Condense Options dialog box opens. Do one of the following

   - To run the operation now, click the **Now** button. At the prompt, click Yes.
   - To schedule the operation to run at a later time, click the **Schedule** button.

Backing Up Server and Volume Settings

In addition to backing up the data on the Snap Server, you may also back up its system and volume settings. The Disaster Recovery screen allows you to create the files you need to recover the Snap Server's configuration settings, and then later, to apply the files in the course of a recovery operation to restore system-wide configuration information, such as network and RAID configurations, as well as volume-extended attributes, such as file and folder permissions and quota information.



The Disaster Recovery Files

Details on the Snap Server Disaster recovery files and the information they contain are as follows:

- **SnapDRImage —** The Snap Server Disaster Recovery Image saves server-specific settings such as server name, network, RAID, volume and share configuration, local user and group lists, and Snapshot schedules. There is one SnapDRImage file per server, residing on the root directory of the first volume at the following path: *server_name**volume_name*

  Tip The SnapDRImage is in binary form and can be safely used only with the Snap Server Disaster Recovery tool. Other tools will not work and may compromise the integrity of the file.

- **Volume-specific files: backup.acl, backup.qta.groups, and backup.qta.users** These files preserve volume-specific settings such as extended ACLs and quota settings. There is one set of these files per volume, residing at the following path: *server_name**volume_name*\.os_private.

Tip The Create Recovery Files option in the Snapshot feature automatically updates the volume-specific files at the time the Snapshot is taken. If you do not use Snapshots to back up a volume to tape, you must manually regenerate these files whenever you change ACL or quota information to ensure that you are backing up the most current volume settings.

Creating the SnapDRImage and Volume Files

Before you create the disaster recovery files, make sure you have completed the following activities:

- You have completely configured the Snap Server. If you subsequently make any major changes to the configuration, the procedures described in this section will have to be repeated.
- You have recorded, in an off-server location, the following information about the configuration: (1) the server name; (2) the number of RAID sets; (3) the number of volumes; and, (4) the size of each volume. You may need to enter this information later as part of a disaster recovery operation.
- You have devised and implemented a data backup strategy as described in the previous section.

To Create and Manage the Disaster Recovery Image and Files

1 **Create the disaster recovery files.**

Navigate to the **Maintenance > Disaster Recovery** screen. Click **Create Recovery Image** to create the SnapDRImage file and the volume files in a single operation.

2 **Copy the files to a safe place off the server.**

Copy the files to a safe location on another server or backup medium. (See page 114 for file names and paths). This strategy ensures that if the file system on the Snap Server is corrupted, the image file will be available to restore server settings.

3 **Take no action regarding the volume-specific files.**

These files will be copied to tape as part of your regular volume backup procedures.

Disaster Recovery Procedures

Caution The procedures described in this section for responding to a catastrophic event are general in nature, and may result in the loss of data. Should such an event actually occur, the exact procedure to follow will vary according to environmental conditions. Snap Appliance strongly recommends you contact a technical service representative before proceeding.

This section describes a worst-case scenario: (1) the operating system has failed, perhaps due to a malicious attack to the root file system, and you cannot access the server; and, (2) the data has been corrupted, and must be restored from tape. When you attempt to connect to the server, the Administration Tool does not appear; instead, the maintenance mode page opens.

About Maintenance Mode

You will encounter the Snap Server maintenance mode only when the GuardianOS has been compromised and is in need of repair or reinstallation. Maintenance mode consists of a series of HTML screens that allow you to perform the following functions:

- **Repair —** Applies the GuardianOSImage but preserves system settings
- **Upgrade —** Upgrades the GuardianOS from one version to another
- **Reinstall —** Reinstalls the GuardianOS, overwriting any previous configurations, and prompts you for the SnapDRImage file
- **Fresh install —** Reinstalls the GuardianOS, overwriting any previous configurations

Tip To install the GuardianOS, you must obtain the appropriate GuardianOSImage file. This file is available from the Snap Appliance Web site.

Performing a Fresh Install in Maintenance Mode

If the GuardianOS has been compromised, the initial maintenance mode screen will appear when you attempt to connect to the server. Use the following procedure to reinstall the operating system.

Caution A fresh install overwrites all data on the Snap Server. Do not perform this operation until all data-recovery attempts have been completed.

1. **Download the GuardianOSImage using one of the following methods:**
   - Click **Browse** to locate and select the file locally.
   - Enter a remote path (FTP, HTTP, etc.) to the file.
2. **Select the Fresh Install option, and click OK.**

This operation may take a few minutes. As the operation progresses, the screen reports the progress of the operation. When the operation is finished, scroll to the bottom of the screen, and click **Continue**. The Continuing Fresh Install Operation screen opens.

3 **When the Fresh Install operation is finished, click Reboot.**

Rebooting takes about three minutes, after which you can refresh the screen by clicking the **Home** icon in the upper right corner of the screen. The Enter Network Password dialog box opens.

4 **Log into the Snap Server.**

Use the default admin, admin user name and password.

5 **Complete the Setup Wizard as described on page 30.**

Make sure to enter the original server name, then reboot the server.

Manually Creating the Original RAID Sets and Volumes

Before you can restore data from tape, you must manually create the same number of volumes as in the original configuration, and each volume must have the same or more space as the originals. The processes summarized below are described in detail starting on page 60.

1 Navigate to the **Storage > RAID Sets** screen and click **Create RAID Set**. Using the screens that follow, recreate the original RAID configuration.

2 Navigate to the **Storage > Volumes** screen and click **Create Volume**. Using the screens that follow, recreate the original Volume configuration.

3 Navigate to the **Storage > Shares** screen and click **Create Share**. Using the screens that follow, recreate the original share configuration.

Restoring the Data from Tape

If you are using Backup Express for GuardianOS, you must restore the catalog to the first volume before proceeding to restore data from tape (for instructions, see "To restore the catalog" on page 113). Users of other backup software packages may require variations in this procedure.

1. **Determine the restoration procedure for your backup software.**

   Refer to your backup software's documentation for details on the appropriate restoration procedure.

2. **Restore only to individual shares within the /shares directory.**

   For example, to restore to the default SHARE1, restore to /shares/SHARE1. If you restore to the /shares directory itself (or to any other place on the root file system), the GuardianOS will be compromised, and you will have to reinstall the OS again.

3. **Restart the server.**

Recovering the Original Server and Volume Configurations

To restore the original configurations to the server, navigate to the **Maintenance > Disaster Recovery** screen in the Administration Tool. Two separate operations are required. They must be run sequentially. After you start any of the recovery processes, you will see the Disaster Recovery Status screen. Do not try to navigate back from this screen during the recovery process. You are restricted to this screen so that you will not interrupt the recovery.

1. **Restore server settings.**

   Click **Recover Server** to open the Server Recovery screen and use the **Browse** button to locate the SnapDRImage file. Click **Recover and Reboot** to start the operation. Once the server configuration recovery operation is complete, you can start the volume configuration recovery operation.

2. **Restore volume ACL and quota configurations.**

   Click **Recover Volume** to open the Server Recovery screen. Select all volumes. (Volumes that do not have a recovery file attached will appear as unavailable, and the corresponding check box is removed.) The creation date of the recovery file on a volume indicates when the recovery image was generated. Click **Recover** to start the operation.

Recovering from Hardware Failures (Snap Server 14000 Only)

This section contains procedures for recovering from hardware components on the Snap Server 14000 only. Procedures for hot swapping disk drives, which also applies to other Snap Servers, appear on page 70.

Chassis Failure

The chassis includes the backplane. In the unlikely event that the chassis of your Snap Server 14000 fails, you can transfer its drives to another Snap Server. Only a qualified Snap Appliance service technician can replace a failed chassis.

Hot Swapping Fans and Power Supply Modules

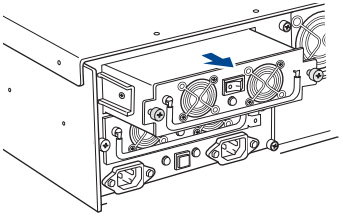
Occasionally, a power module or fan unit may fail. To recover from this type of failure, hot swap the failed device within the server. Use the following procedures to replace failed components.

Hot Swapping a Power Supply Module

The Snap Server 14000 power supplies are fully redundant. Powering down a single module will not interrupt system availability. When a power supply module fails, the indicator light on the failed module glows amber. The front LCD status display also indicates that a module has failed.

Caution Never remove a power supply module while it is still powered on because it may crash your system. Always turn the power module off before swapping it.

To Replace a Failed Power Supply Module



1. Turn the on/off switch to the **off** position.
2. Unscrew the thumbscrews on each side of the power module.
3. Pull on the handle to remove the failed power module.
4. Turn the on/off switch to the **off** position on the replacement power module.
5. Insert the new power module and fasten the thumbscrews.
6. Turn the on/off switch to the **on** position on the replacement power module. The indicator light should be green.

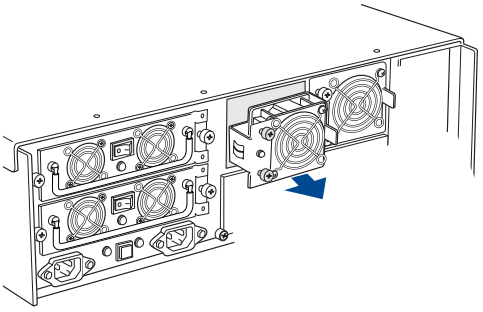
Power Supply Module Indicator Lights

A second set of power supply module indicator lights is located below the two power supplies: a green light and an amber light. The green light is continuously lit when the power supplies are active and working properly. A blinking green light indicates that one of the power supply modules is not active. The amber light comes on when a module is not functioning properly.

Hot Swapping a Failed Fan

When a fan fails, the indicator light on the failed module glows amber. The front LCD status display also indicates that a fan has failed.

1. Unscrew the thumbscrews on the fan.
2. To remove the failed fan, use the small tab handle to pull the fan out.
3. Insert the new fan and tighten the thumbscrews.



Chapter 7

Monitoring and Maintaining Snap Servers

This chapter describes how to use the Administration Tool to monitor and maintain a Snap Server. It includes information on configuring e-mail notification, *e*Trust Inoculate*IT*, SNMP, accessing server status information, viewing the event log, and resetting server settings to factory defaults.

- **Configuring E-mail Notification —** Provides requirements and options for configuring e-mail notification for system events.
- **Simple Network Management Protocol (SNMP) —** Provides information on default traps and instructions of using SNMP to monitor the Snap Server.
- **Using Status Screens —** Lists status screens available in the Administration Tool for monitoring overall system status, volume statistics, and backup device status.
- **Using the Event Log —** Explains the usage of the Event Log. an overview of the Snap Server's antivirus protection features and configuration options.
- **Resetting the Snap Server to Factory Defaults —** Explains the three options available for restoring a Snap Server to default values.
- **eTrust InoculateIT —** Provides an overview of the Snap Server's antivirus protection features and configuration options.

Configuring E-mail Notification

To configure the server to send e-mail alerts in response to system events, navigate to the **System > E-mail Notification** screen. To set up e-mail alerts, you will need: (1) the SMTP server's IP address; and, (2) the e-mail address of each recipient who is to receive an alert. You can set up notification for the following events:

- The server reboots due to an automatic or manual process
- A RAID 1 or 5 experiences a disk drive failure or a disk drive is removed (degraded)
- A RAID 1 or 5 configures a spare or a new disk drive as a member (rebuilds)
- Storage space on a volume reaches 95% utilization
- The internal temperature for the server exceeds its maximum operating temperature

Simple Network Management Protocol (SNMP)

SNMP views a network as a collection of cooperating, communicating devices that consists of managers and agents. The Simple Network Management Protocol monitors and manages network devices, such as computers, routers, bridges, and hubs.

The Snap Server can act as an SNMP agent. SNMP managers collect data from agents and configure the data. Agents respond to managers and may also send traps, which are alerts that indicate error conditions. The server communicates with SNMP managers in the same community. A community name is a password that authorizes managers and agents to interact. The server only responds to managers that belong to the same public or private community.

Default Traps

A *trap* is a signal from the Snap Server informing an SNMP manager program that an event has occurred. The Snap Server supports the following default traps:

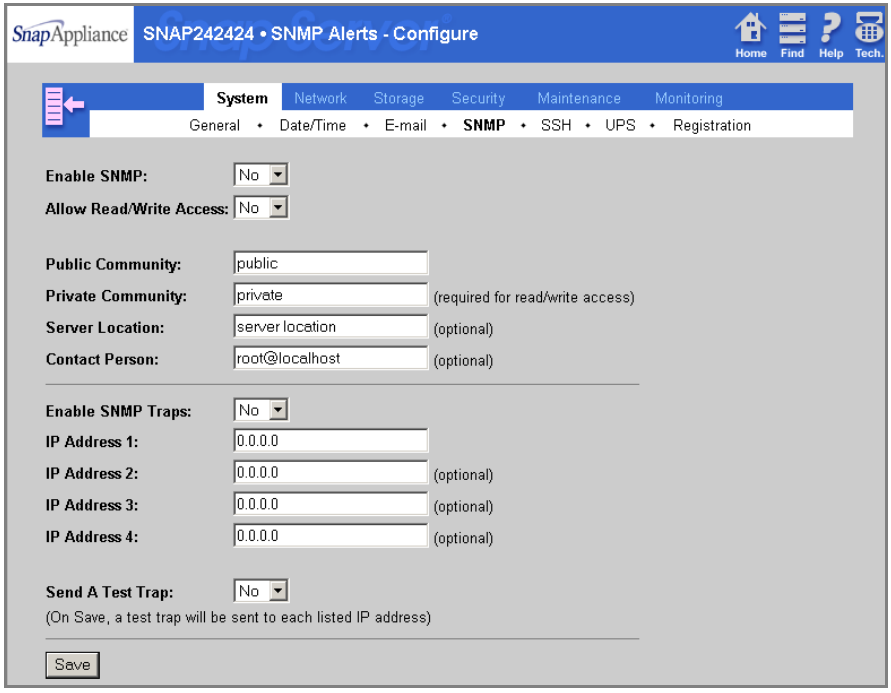
- **coldStart** — An SNMP agent has restarted
- **linkDown** — An Ethernet interface has gone off-line
- **linkUp** — An Ethernet interface has come online
- **authenticationFailure** — An attempt to query the SNMP agent using an incorrect public or private community string was made, and resulted in a failure
- **enterpriseSpecific** — Snap Server-generated traps that correspond to the error-level, warning-level, and fatal-error-level traps of the GuardianOS. These traps contain a descriptive message that helps to diagnose a problem.

Supported Network Manager Applications

You can use any network manager application that adheres to the SNMP V2 protocol with the Snap Server. The following products have been successfully tested with Snap Servers: CA Unicenter TNg, HP Open View, and Tivoli NetView.

Configuring the Server for SNMP

To configure the Snap Server as an SNMP agent, navigate to the **System > SNMP** screen. Once enabled, SNMP managers can access MIB-II and Host Resources MIBs management data on the server.



1 To enable SNMP, select *Yes* in the pull-down menu.

2 Complete these fields as appropriate:

- **Allow Read/Write Access —** Select *No* to allow SNMP managers to collect data from the server. Select *Yes* to allow SNMP managers to collect data and to configure MIB variables on the server.
- **Public Community —** To enable SNMP managers to read data from this server, enter the name of one or more public communities, or accept the default public.

- **Private Community —** To enable SNMP managers to remotely configure this server, enter the name of one or more private communities, or accept the default private. Create unique public and private names. As a precaution against unauthorized access, Snap Appliance recommends that you create your own public and private community names.
- **Server Location —** Enter information that helps a user identify the physical location of the server. For example, you might include a street address for a small business, a room location such as *Floor 37, Room 308,* or a position in a rack, such as *rack slot 12*.
- **Contact Person —** Enter information that helps a user report problems with the server. For example, you might include the name and title of the system administrator, a telephone number, pager number, or e-mail address.

3 To configure traps, complete the screen parameters as follows:

- Select *Yes* to enable traps.
- Enter the IP address of at least one SNMP manager in the first field as a trap destination. You can enter up to three additional IP addresses.
- To verify your settings, select *Yes* in the Send a Test Trap pull-down menu.

4 Click **Save**.

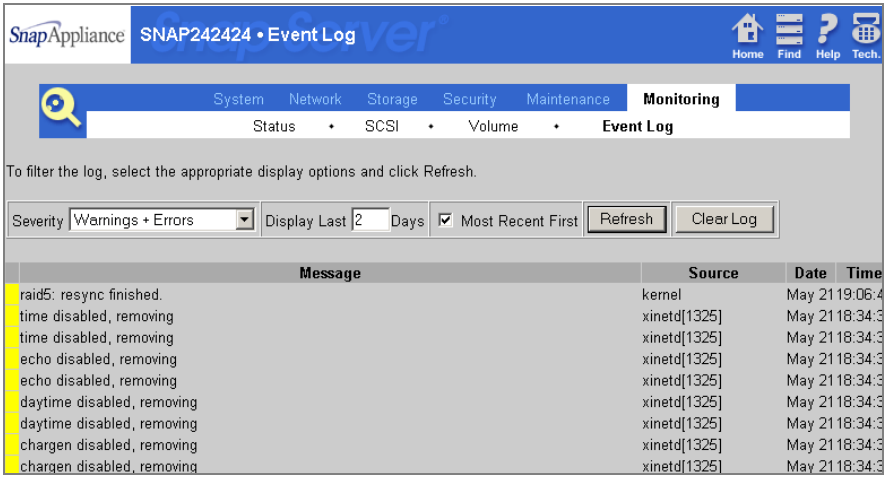
Using Status Screens

Snap Servers provide a number of read-only screens that report on the status of various components.

- The **Monitoring > Status** screen provides miscellaneous system data.
- The **Monitoring > SCSI** screen displays a list of all SCSI devices found attached to the Snap Server. Backup applications such as Backup Express for GuardianOS require you to enter this information as part of the configuration process.
- The **Monitoring > Volume Usage** screen displays summary information about each volume, including name, RAID level, capacity, free space, utilization, and volume status.

Using the Event Log

Use the **Monitoring > Event Log** screen to view a summary of all operations performed on the server. Yellow indicates a caution, red indicates an error, and blue indicates information.



You can control the appearance of this screen using the following controls:

- Use the controls along the top of the screen to select the severity level, time range, and order of events displayed.
- Click **Refresh** to update the Event Log.
- Click **Clear the Event Log** to erase all log entries.

Resetting the Snap Server to Factory Defaults

The GuardianOS allows you to reset different components of the system. Default settings can be found in the default configuration sections of chapters 3, 4, and 5.

Caution Each reset option requires a reboot of the server. To prevent possible data corruption or loss, make sure all users are disconnected from the Snap Server before proceeding.

1. Navigate to the **Maintenance > Factory Defaults** screen, and select one of the following options.
   - The **Reset Network Configuration to Factory Defaults** option returns TCP/IP and other protocol settings set in the Network tab to factory defaults (see "Default Networking Configuration" on page 38).
   - The **Reset System Settings, Network, and Admin Passwords to Factory Defaults** option returns the admin and root passwords to the default value, returns TCP/IP and other protocol settings set in the Network tab to factory defaults, eliminates all shares to all volumes except for a single share to the root of each volume, and returns settings for server name, date and time, users, groups, and the activation and configuration of *e*Trust Inoculate*IT* to factory default values.

     When the server finishes rebooting, the login dialog box opens. Enter the default admin password of admin, and click OK. The Initial Setup Wizard runs, allowing you to reset most of these options.
   - The **Set Default ACLs for Volumes** option resets the file and directory ACLs on selected volumes to reset the Everyone group to full control. Essentially, all users will be able to access all directories and files after the reset (within the confines of share access settings). This reset option allows administrators to clear away residual file-level ACL settings that may no longer be necessary under the security enhancements included in the GuardianOS 2.4 release.
2. Click **Save**.

*e*Trust Inoculate*IT*

The Computer Associates antivirus software is a powerful antivirus solution that is preinstalled on all Snap Servers. The software, certified by the International Computer Security Association (ICSA) to detect 100 percent of viruses in the wild, uses a rule-based, analytical virus scanner to detect known viruses. By default, the *e*Trust Inoculate*IT* software is enabled on Snap Servers, but no scan jobs or signature update schedules are configured.

Components

- **Java-based User Interface —** The eTrust browser interface can be accessed through from the Snap Server Administration Tool. Use this graphical user interface (GUI) to perform all antivirus configuration and management tasks. This GUI provides access to detailed instructions in the online help.

  Caution The Java implementation provided with Internet Explorer does not fully support the eTrust Java-based interface. To resolve this issue, install a current version (v1.3.1 or higher) of the Java 2 Platform, available for download from http://java.sun.com.

- **Local Scanner —** A rule-based scanning engine that runs on the Snap Server detects known viruses. Unknown viruses are detected using the Heuristic Scanner option.
- **Scheduled Scanner —** Use the Schedule Scan Job options to automate scanning so that the scan runs at a specific date and time, and optionally at repeated intervals.
- **Log Reports —** A sophisticated reporting mechanism logs all scanning operations, which can be reviewed for tracking and analysis. Use the Log Viewer to view and manage logs for each type of scan operation, to view signature update log information, and to view and modify scheduled scan options.
- **Signature Updates —** Signature updates are made available on a regular basis by Computer Associates. With a few simple configuration tasks, you can automate antivirus protection on a Snap Server. All signature updates, distribution, monitoring, scanning settings, and scanning operations can be configured to run with no administrator intervention and no downtime on the server.

Local Scanner and Log Views

The eTrust browser interface offers two views (or modes) that display different administrative functions: 1) the default *Local Scanner* view provides scheduling and scanning options; and, 2) the *Log Viewer* view allows you to view and manage the scanning activity logs. To change views, select the desired option from the View menu. (A third view, the *Administrator's View*, is not available for Snap Servers.)

Configuration Options Available in Local Scanner View

All options that are supported by the GuardianOS are enabled in the Scanner menu. These include:

- Local Scanner Options
- Signature Update Options
- Contact Options
- Alert Options
- Service Manager

Configuration Options Available in Log Viewer View

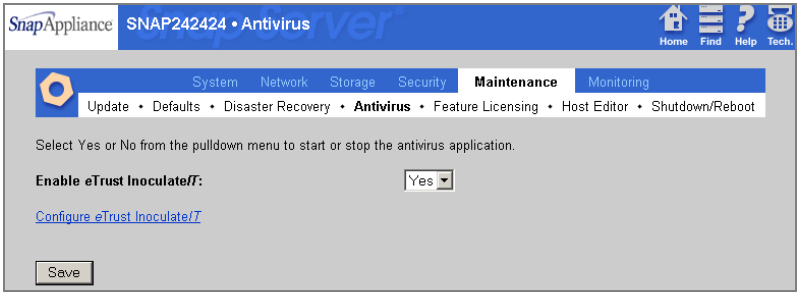
All options that are supported by the GuardianOS are enabled in the Log menu. These include:

- Local Scanner
- Scheduled Scanner
- General Events
- Distribution Events

Launching the eTrust Antivirus Browser Interface

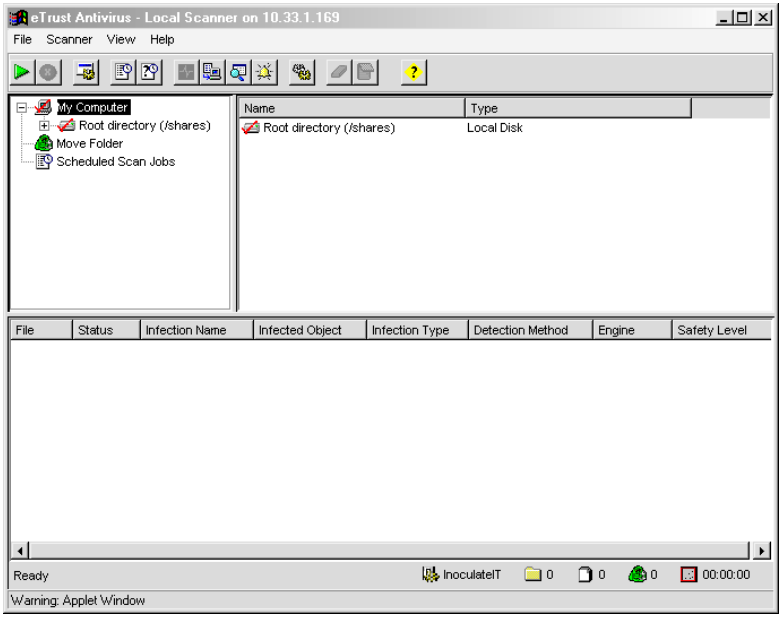
To launch the eTrust browser interface, use the following procedure.

1 Navigate to the **Maintenance > Antivirus** screen in the Administration Tool.



2 To launch the Configuration GUI, click the **Configure *e*Trust Inoculate*IT*** link. The *e*Trust Inoculate*IT* splash screen appears. The first time you connect, it may take from 30 seconds to several minutes for the GUI to load, depending on the speed of your connection.

3 The CA Antivirus Security Login dialog box appears. Enter the same admin user name and password (case-sensitive) you have established for the Administration Tool, and then click **OK**. The eTrust GUI opens to the Local Scanner View.



Caution The Internet Explorer Java implementation does not fully support the eTrust antivirus interface. To resolve this issue, install a current version (v1.3.1 or higher) version of the Java 2 Platform, available for download from http://java.sun.com.

Using the Local Scanner

The Local Scanner assures comprehensive antivirus protection for a Snap Server by providing you the ability to scan for infections on demand. You can use the Local Scanner on a Snap Server whenever you want to check for infected drives, folders, files, or disks. Before you run a scan you can set options for managing an infected file so that after you start the scan no further action is required. You can also set options to only report on the occurrence of an infection. This allows you to decide what action to take after the infection is found.

Subsequent sections briefly describe the main features of the Local Scanner; see the online Help for detailed descriptions of all of the Local Scanner options and procedures for using these features.

The Local Scanner Window

The Local Scanner window displays a list of items available for scanning on the left side of the window, and displays the contents of a selected item on the right side of the window. You can set options for what is displayed, and for how to manage scanning on the Snap Server.

The Scanning Options Dialog Box

To set scanning options, choose the **Scanner > Local Scanner Options** command. The Scanner Options dialog box that opens consists of five tabs:

- Scan
- Selection
- Display
- Directory
- Log

When you specify options for a scan, you indicate how the scan is performed and what actions to take if an infection is found. Whether you perform a local scan or a scheduled scan, you can choose different settings for each type of operation. For example, file action options control what happens when an infection is found. When you perform a local scan, you might have the file action set to *Report Only*. When you set options for a scheduled scan, you might have the file action set to *Cure File*.

Tip You may not want to include Snapshot shares (see "Using Snapshots" on page 98) as part of your virus scan. Because access to an archived version of the file system provided by a Snapshot share is read-only, you cannot treat or move any infected file; you would have to delete the entire Snapshot to effect a cure. A more useful approach is to always scan your file system for viruses before running a Snapshot. Adjust your antivirus scan schedule to synchronize with your Snapshot schedule such that any infected files are cured or removed before the Snapshot is scheduled to fire.

Setting the Scan Options

Scan options are displayed on the Scan tab of the Scanner Options dialog box. Use these options to change the scan level, change the scanning engine or detection options, and to control how to treat an infection if one is found. These options can be used for both local scanning and scheduled scanning.

Safety Level — You can set the scan safety level to *Secure* or *Reviewer* mode. Use the Secure mode as the standard method for scanning files completely. If you suspect you have an infection that is not being detected by the Secure mode, you can use the Reviewer mode. Use the Reviewer mode to detect viruses that are inactive or have been deliberately modified. Note that Reviewer mode runs significantly slower than Secure mode.

Scanning Engine — The scanning engine is the specialized processor that does the work of looking for infections. The only choice available by default on the Snap Server is *e*Trust Inoculate*IT*.

Advanced Options — You can click the **Advanced** button to enable the Heuristic Scanner engine, which scans files for viruses whose signatures have not yet been isolated and documented.

File Actions — You can set these options before you run the scan or after you run the scan. If you want to see if there are any infections before you decide what to do with an infected file, choose *Report Only*. If an infection is found, you can then choose any of the other actions. The following file actions are available.

File Actions	Description
Report Only	Reports when an infection is found.
Delete File	Deletes an infected file.
Rename File	Renames an infected file with an AVB extension. Infected files with the same name are given incremental extensions in the form #.AVB (e.g., FILE.0.AVB, FILE.1.AVB, and so on). After a file is renamed with an AVB-type of extension, it is not scanned subsequently.
Move File	Moves an infected file from its current directory to the Move directory for quarantine.
Cure File	Attempts to cure an infected file automatically. Choosing this setting enables the **File Options** button. Click this button to display the Cure Action Options and specify how the Cure File option performs. Note that the System Cure option is not available on Snap Servers.

Setting Selection Options

Selection options are displayed on the Selection tab of the Scanner Options dialog box. Use the Selection options to choose the types of objects to scan, the types of file extensions to include or exclude from a scan, and the types of compressed files to scan.

Objects to Scan — You can only choose the *scan files* setting on the Snap Server. When you scan files, the types of files that are scanned are determined by the types of extensions you select to include or exclude, as indicated by the Regular Files and Compressed Files options

Regular Files — You can choose to scan files regardless of extension, or select specific types of extensions to include or exclude.

Compressed Files — To scan compressed files, you must select the *Scan Compressed Files* setting, and then click the **Choose Type** button to specify the compressed file extension types. You can set additional options for the that improve scan performance by clicking the **Options** button.

Setting Display Options

Display options are shown on the Display tab of the Scanner Options dialog box. Use the Display options to specify the types of drives and files to display in the Local Scanner window. With these options you can tailor the display of objects so that you see only the types of interest to you.

- **Drives —** On Snap Servers, all mounted file systems are always selected for display.
- **Files —** You can select to display only the types of files that you want to see in the Local Scanner window. You can show all files, or hide files based on the file extensions that you specify using the selection filters on the Selection tab.
- **Show Summary after Scan Completes —** Select this option to automatically display the Scan Result Summary when a scan is finished. This summary includes information on the time the scan started and stopped, the number of files scanned, the number of infections found, the number of infections cured, and other statistics on file actions.

Viewing Directory Paths

Directory paths are displayed on the Directory tab of the Scanner Options dialog box. The Directory options display the locations of the directories used by the antivirus software. In addition, the Rename Extension is displayed.

Filtering File Information for Logs

Log filter options are displayed on the Log tab of the Scanner Options dialog box. You can specify the types of events that are written to a log. Use the Filter options to specify whether or not information about a file is written to the list in the log. These options allow you to tailor your scan logs for the type of information you need. You can record information about the following:

- Infected files
- Clean files that are examined and found not to be infected
- Files that are skipped and not scanned

Check the Infected files option to put information in the log about files that are found to be infected. Check the Clean files option to put information in the log about files that are scanned and are not infected. Check the Skipped files option to put information in the log about files that have been excluded from the scan.

About Signature Updates

Signature updates contain the latest versions of the signature files that recognize and defend against the latest infections. They also contain the latest engine versions, which do the work of looking for infections. Computer Associates provides regularly scheduled signature updates every month, and more frequently as needed.

When you set up a signature update, you specify when to perform the update and how to collect it. You can collect signature updates via FTP or from a path on the local machine.

These updates are cumulative, so they contain everything from all previous file updates, plus the newest information on the latest infections. If you have missed a recent update, you only need to collect the latest signature file to have the most up-to-date protection.

Setting Signature Update Options

To set signature update options, choose **Scanner > Signature Update Options**. The Signature Update Options dialog box that opens consists of three tabs:

- Schedule
- Incoming
- Outgoing (These options are not supported on the Snap Server.)

Use these options to set up when to collect the signature updates, where to get them, and which engine versions and platforms to include.

The signature updates that are appropriate for your configuration are available by default. Snap Servers are preconfigured to get signatures via ftp from ftpav.ca.com. To update a server, you simply use the Schedule tab to set a time for the signature update job (or you can get the signatures immediately).

Setting Schedule Options

Use the Schedule tab to enable scheduled downloads, and to specify the date, time, and repeat values for the signature update. You can schedule a signature update job to download the signature update immediately, or schedule the signature update job to run once or repeatedly at specified time intervals.

Download Now — Use this button to perform an immediate signature update job. The settings on the Incoming tab (see following section) are used for this job.

Enable Scheduled Download — Use this option to indicate that scheduled automatic downloads will be done. To have the signature updates distributed automatically on a machine, you must invoke this option. When this option is not in effect, the scheduled download feature is disabled.

Download Date and Time — Use the Date option to specify the month, day, and year for the job. The drop-down arrow displays a calendar you can use to select a date. Use the Time option to specify the time of day for the job, in hours and minutes.

Repeat Every — Use these options to specify how often to run a periodic signature update job. You can schedule a signature update job to run at a regularly scheduled time, in months, days, hours, or minutes.

Setting Incoming Options

Use the Incoming tab to define the sources of signature updates. The Download Sources List displays sites from which you can download signatures. Snap Servers are preconfigured to get signatures via ftp from ftpav.ca.com.

Add — Click this button to display the Source Select dialog, in which you can add a download method and a source for the update to the list. The available methods are as follows:

Method	Description
FTP	Use FTP to download the update files from the Computer Associates FTP site. You can also use FTP to distribute signature updates from one Snap Server to another. Note that when using FTP, the user name and password are passed as clear text.
UNC	Use UNC to distribute signature updates from one Snap Server to another. Note that for UNC to work, on the Snap Server on which the signature updates reside, you must have Enable Guest Account option set to *Yes* (**Security > Windows**).
Local Path	As part of the procedure to provide signature updates to a Snap Server with no Internet access, you can connect to a local share on the Snap Server. Note that the path to the share is case sensitive.

Perform Fast Download — Use the Fast Download option to bring your signatures up to date without downloading information you already have. When this option is selected, the download process analyzes your current signature information to determine what kind of update you need. If you only require an incremental update of the data files, then the appropriate files are downloaded and updated automatically. If an incremental update is not appropriate and a full update is necessary, then all the signature and engine files are downloaded and updated.

Updating Snap Servers That Have Internet Access

Snap Servers are preconfigured to download signature updates from the CA FTP site at ftp://ftpav.ca.com/pub/inoculan/scaneng. If your Snap Servers have direct access to the Internet, you only need to schedule the downloads (choose **Scanner > Signature Update Options**, and click the Schedule tab) to set up automatic signature updates. If access to the Internet is routed through a proxy server, you may also need to specify the name of the proxy server. To do so, use the following procedure.

1. Choose **Scanner > Signature Update Options**, and click the Incoming tab.
2. Select *FTP* in the list box, and click **Edit**.
3. In the Proxy Name field, enter the IP address of the proxy server, and click **OK**.

Updating a Snap Server That Does Not Have Internet Access

If you have Snap Servers that do not have Internet access, use the following procedures to download the signature files to a machine with Internet access and then copy them to the Snap Server.

1 Using a workstation with Internet access, go to ftp://ftpav.ca.com/pub/inoculan/scaneng and download the following files.

- All *.tar files containing the word *Linux*, e.g., fi_Linux_i386.tar and ii_Linux_i386.tar
- All *.txt files containing the string *Sig*, e.g., Siglist.txt and Siglist2.txt

2 Using a method appropriate to your environment, copy the update files to a Snap Server.

Tip Copy the files to the root of a share. You can configure other Snap Servers to automatically get their signature updates from a single Snap Server (see following procedure). To do so, the update files must reside on the root of a share, not a subdirectory within a share.

3 Choose **Scanner > Signature Update Options**, and click the Incoming tab.

4 Click the **Add** button, and select *Local Path* from the Method pull-down menu.

5 In the Path field, enter to path to the directory on the Snap Server in which the update file resides, for example:

/shares/*SHARE1/sigfiles*.

where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.

6 Click **OK**. The path appears in the list box.

7 Select the Local Path, and click **Download Now**.

Distributing Updates from One Snap Server to Another

To Distribute Files via UNC

If you have more than one Snap Server with no Internet access, you can perform the previous procedure on just one of them, and then configure your other Snap Servers to get the update from that Snap Server automatically via UNC.

1. Choose **Scanner > Signature Update Options**, and click the Incoming tab.
2. Click the **Add** button, and select *UNC* in the Method list box.
3. Enter the path to the Snap Server to which the update files have been downloaded (see previous procedure) using the following format:

   *server_name**share_name*

   where *server_name* is the name of the Snap Server, and *share_name* is the name of the share providing access to the files. (The update files must reside on the root of the share.)
4. Click **OK**. The path you entered appears in Download Sources list box.
5. Select the path, and click **Download Now**.

To Distribute Files via FTP

If you have more than one Snap Server with no Internet access, you can perform the FTP download procedure on just one of them, and then configure your other Snap Servers to get the signature updates from that Snap Server automatically via FTP.

1. Choose **Scanner > Signature Update Options**, and click the **Incoming** tab.
2. Click the **Add** button, and select *FTP* in the Method list box.
3. Enter the following information regarding the Snap Server on which the update file resides as follows:
   - In the Host Name field, enter the IP address.
   - In the User Name and Password fields, enter the admin user name and password.
   - In the Remote Path field, enter the path to the directory in which the file resides. For example:

   /shares/*SHARE1/sigfiles*

   where *SHARE1/sigfiles* is the share path to the directory containing the signature update files.
4. Click **OK**. The path you entered appears in Download Sources list box.
5. Select the path, and click **Download Now**.

Understanding Alert Options

This section describes the integrated options in the Computer Associates antivirus software GUI that allow you to set options for managing the information that is passed to the Alert Manager on the Snap Server.

These options allow you to tailor the notification information that is provided to the Alert Manager, cut down on message traffic, and minimize the dissemination of notifications that are not critical. The following tabs are available for the Alert Settings dialogs.

- Report
- Filter

The Report Tab

Use the Alert Report options to specify where to send notification information, and to manage how frequently to send messages. You can specify the following destinations.

Option	Description
Local Alert Manager	Send notification information to the Alert Manager component on the local machine.
Event Log	Send notifications to the system event log of the local machine.
Forward To	Not Supported
Machine Name	Not Supported

Managing Report Criteria

Use the Report Criteria options to manage how frequently messages from the General Event Log are reported, based on the settings for the Report To options. The Queue Up and Time Out After options work together. Messages are reported based on whichever limit is reached first.

Options	Description
Queue Up Records	Use the Queue Up option to specify a number of message records to collect in the General Event Log. When the limit is reached, the information is reported as specified in the Report To options.
Time Out After	After the specified number of minutes is reached, the information in the General Event Log is reported as specified in the Report To options, even if the number of messages has not reached the Queue-Up number.
Skip Older Than Days	Any record in the General Event Log that is older than the specified number of days is not reported.

Setting Alert Filter Options

Use the Alert Filter options to manage notification severity levels, and to customize sets of notification messages to be reported for the different Computer Associates antivirus service components. These options allow you to determine what types of messages should be passed to the Alert Manager. You can use Notification by Level of Severity or Custom Notification.

Notification by Level of Severity

You can choose to send notifications by their level of severity.

- **Informational —** This type of message provides information on events such as if the service has started or stopped and if no infections have been found.
- **Warning —** This second priority message provides non-critical warning information.
- **Critical —** This is the highest level message. It requires immediate attention once logged. This message could mean there is an infection detected, or there is a problem with the service, such as an error loading an engine.

Custom Notification

Use the custom notification option to customize sets of notification messages for the different services. Choose one of the available service modules and select from a list of associated notification messages. Use these options to specify which messages you want to send as notifications. This limits the messages that are reported. For each service module, you can select specific messages that you want reported. The following service modules are available.

- **Local Scanner —** For local scans.
- **Job Server —** For the scheduled scan job and signature update scheduling agent.

Tip The Realtime Server and Admin server settings have no effect on Snap Servers.

List of Notification Messages

For each service selected, a different list of messages is available. The level of severity of each message is listed, along with the text of the message.

You can use this list to select only the messages that you want to be passed to Alert, and in turn, reported by the different methods of communication specified by the configuration options in Alert. By choosing the types of messages, you can cut down on unwanted network message traffic. Only the messages that you determine to be of importance and warranting a notification will be passed along.

Other Local Scanner Options

The following list summarizes other options available in the Scanner menu.

- **Contact Options —** To specify the contact information that is automatically sent when you send a file for analysis, choose the **Scanner > Contact Options** command. In the Contact Information Option dialog box that opens, enter contact information for your firm as appropriate.
- **Service Manager —** The Service Manager provides a convenient way to access the Computer Associates antivirus services running on a Snap Server. Choose the **Scanner > Service Manager** command to display the Manage the Services dialog. From this dialog you can start, stop, and view the status of the services.
  - **RPC Server** is the remote management agent (InoRpc) that provides communication services between machines in the antivirus network.
  - **Job Server** is the scheduled scan job and signature update scheduling agent: InoTask.

Under normal circumstances, you do not need to stop or start these services.

Using the Move Directory

To view infected files, make sure you are in Local Scanner view and click the Move Folder directory on the left of the window. Infected files appear on the right. When a file is put in the Move Folder, it is given a unique name to identify it. Thus, if you had infected files with the same names that were stored in different directories, they remain distinct if they are moved. To manage a moved file, right-click the file and select from the following options:

- **Restore —** This option removes the file from the Move Folder and restores it to its original location with its original name and type.
- **Restore as —** This option displays a dialog box that allows you to change the directory location and file name. You can rename a file and isolate it safely in a different location. You may want to use this option, for example, if you do not have another source for the data and you need to look at the file. Or you may have a file that you want to analyze.

  Tip To restore a file to different directory, you must prepend the path to the directory with the string /shares. For example, to restore a file to the SHARE1/sales directory, enter the path as follows:
  /shares/SHARE1/sales
- **Restore and Cure —** This option allows you to restore the selected item back to the original folder it was in, and cure it. This option is useful if you update the signature files after items have been put in the Move folder. If a cure is provided that you did not have available, you can get the latest signature update and use this option to restore and cure an infected item.
- **Delete —** This option deletes the infected file; no warning or confirmation message is displayed.

Using the Log Viewer Window

Use the Log Viewer window to select, view, and manage the scanning activity logs. The Log Viewer window displays a list of different log categories on the left of the screen. Select a directory to display a summary list of the available logs on the right of the screen. Logs are listed by date and time they were created.

When you right-click an item in the Log Viewer, different options are available to delete, print, view properties, or refresh the display of the log information.

The Log Viewer List

The Log Viewer list can contain logs for the following categories of scan jobs.

- **Local Scanner —** This directory contains a list of logs that report the results of the scan jobs that have run on your Snap Server.
- **Scheduled Scanner —** This directory contains a list of scheduled scan jobs. For each job, there is a scan log that contains the results for each time that the job has run, listed by the scheduled date and time. If a job only runs one time, you have one result log. If the job runs periodically, there is a unique result log for each scan job.
- **General Events —** This directory contains logging information of general events for each day. Operating system error codes can also be seen here. The following types of messages can be displayed.

Message	Description
Critical Message	The highest level message. It requires immediate attention once logged. This message could mean there is a virus detected, or there is a problem with the service, such as an error loading an engine.
Warning Message	This second priority message provides non-critical warning information.
Informational Message	Provides information on events such as if the service has started or stopped and if no viruses have been found.

- **Distribution Events —** This directory contains logging information of signature update distribution events for each day. Events are recorded for any actions that occur during the signature update and distribution process. This includes details about connecting to a signature distribution source, starting and stopping a download, and information about whether the signature files have been downloaded successfully.

Chapter 8

Troubleshooting

This chapter describes common troubleshooting suggesting regarding installation, networking, security, and data protection issues. For more troubleshooting tips, visit the Snap Appliance Web site at http://www.snapappliance.com/support.

Networking Issues

Problem: The server cannot be accessed over the network.

Solution: Inaccessibility may be caused by a number of reasons. To resolve this issue, use one of the following methods:

- Verify that you have the correct IP address of the server, and try to connect again.
- Verify that the amber LED for the primary Ethernet port is lit. (This light indicates network connectivity). If the light is not lit, the most likely cause is a mismatch between the settings on the switch or hub and the settings on the Snap Server Ethernet port. These settings must match. To resolve the problem, make sure that the port settings on the hub or switch match the settings for the primary port as configured on the **Network > TCP/IP** screen of the Administrator Tool. Using the autonegotiate setting on both the switch and the server port.

Problem: The Snap Server does not operate properly on a network running Gigabit-full duplex.

Answer: For Gigabit Ethernet to operate properly, both the switch and the Snap Server's primary Ethernet port (Ethernet1) must be set to *Auto* (autonegotiate). Any other setting will result in unexpected behavior and reduced performance.

Problem: The network does not have a DHCP server and the Snap Server IP address is unknown.

Answer: Install NASManager from the Snap Server User CD onto a client workstation. You can then use the utility discover all Snap Servers on your network, and to assign a static IP addresses as necessary.

Problem: Apple users cannot log on to the Snap Server as Windows users.

Solution: To allow Apple users to access a Snap Server, you must replicate their user names and passwords locally on the Snap Server.

Using Maintenance Modes

Some troubleshooting issues can be solved using the Snap Server's maintenance modes. These functions allow you to perform basic server functions when network connectivity has been cut off. On the Snap Server 14000, all six modes are available from the LCD. On Snap Servers 4200, 4400, and 4500, pressing the reset button results in the actions described for modes 1 and 6. The six maintenance modes are:

- **Mode 1 —** Restores default TCP/IP settings (DHCP)
- **Mode 2 —** Restores the admin account to a user name and password of admin, admin
- **Mode 3 —** Resets network settings to factory defaults
- **Mode 4 —** Resets system settings to factory defaults
- **Mode 5 —** Reserved for technical support
- **Mode 6 —** Boots the system to a series of HTML screens that allow you to repair or reinstall the Snap Server operating system.

To Run the Snap Server 14000 in Maintenance Mode

1. Power off the server.
2. Depress the middle button (under the LCD panel) and power up the server, keeping the middle button depressed until maintenance mode 1 displays in the Snap Server's LCD.
3. Use the buttons to navigate to the desired maintenance mode.

To Run Snap Servers 4200, 4400, and 4500 in Maintenance Mode

To reset the server's IP address to the default (DHCP) and enter maintenance mode, do the following. With the server powered on, go to the rear of the Snap Server 4400 and press the reset button located near the Ethernet ports (you will need a small

tool such as a pen or pencil to press the button). On the 4200 and 4500, remove the front bezel and press the white button, located to the left of the black power button. The system will reboot, and after about a minute, the system light should begin to alternately flash amber and green. When you next access the server, the initial maintenance mode (Recovery Console) screen opens.

This will change the Snap Server's IP address. To access the Recovery Console screen, you will need to know the IP address of the Snap Server. You can find the server's IP address from the DHCP server on your domain. If you do not have a DHCP server, the server's IP address should default to 10.10.10.10. If so, you will need to change the IP address on the client you are connecting from to the same network segment as the Snap Server, (i.e. 10.10.10.5) to access the Recovery Console.

Disaster Recovery and Maintenance Issues

Problem: I backed up my Snapshot share and I am now attempting to restore it, but the operation is failing.

Solution: A Snapshot share is read only. You can restore the data to a read/write accessible share.

Problem: Power to the Snap Server was unexpectedly cut off due to a power outage.

Solution: Snap Appliance recommends that you use an uninterruptible power supply (UPS) with the Snap Server. If you did not have a UPS attached to the server at the time of the power outage, use the following procedure:

1. Turn off the power supplies (one on Snap Servers 4200, 4400, and 4500; two on the Snap Server 14000) and leave them off until the power situation stabilizes.
2. Once the power is restored and stabilized, turn the power supplies back on and reboot the server.

   Once the Snap Server boots, it begins resynchronizing the RAID(s). You can use the server during the resynchronization, but performance will be a little slower than normal. Do not remove drives, however, while the server is resynchronizing the RAID.

Problem: The server is not responding to file requests or configuration commands.

Solution: Call your Snap Appliance technical support representative.

Problem: The admin password to the Administration Tool is not available.

Solution: Use one of the following methods as appropriate.

- Snap Server 4200, 4400, and 4500: Press the Reset button on the Snap Server to reset the admin password to the default setting of admin. (Pressing the Reset button also boots the system into Maintenance mode).
- Snap Server 14000: Use Maintenance Mode 2 to clear the administrative password, then use the Administration Tool to set a new password.

Problem: I am located in corporate headquarters where I used the server for several months. Recently, I sent the server to a satellite office. I forgot to clear the system settings.

Solution: You can resolve this problem in several ways:

- Install NASManager at the new location. Change the IP address and set a new administrator password. You can then use the Administration Tool to set up new preferences.
- Snap Server 14000 Only: Use Maintenance Mode 4 to clear all the system settings. Run the Administration Tool to set up new preferences.

Problem: The Snap Server 14000 LCD is flashing rapidly.

Solution: A rapidly flashing LCD indicates a server panic. In some cases, rebooting the server may solve the problem. However, if this condition occurs more than once, contact Snap Appliance technical support.

Problem: The Snap Server has been compromised and cannot be accessed over the network.

Solution: Use maintenance mode to reestablish basic connectivity to the Snap Server.

NASManager Installation Issues

Problem: On a Windows 2000 client the NASManager installation program seems to hang when the process reaches 99 percent completed.

Solution: Windows requires two to three minutes *after* reaching the 99 percent completed mark to finish installing NASManager.

Appendix A

Snap Server Specifications

This appendix contains specifications for the Snap Server 4200, 4400, 4500, and the Snap Server 14000. Specifications are subject to change without notice. Up-to-date specifications are posted at http://www.snapappliance.com.

GuardianOS Specifications

These specifications apply to all Snap Servers running the GuardianOS.

Feature	Specification
Network Transport Protocols	TCP/IPAppleTalk
Network File Protocols	Microsoft (CIFS/SMB) UNIX (NFS) Apple (AFP) Internet (HTTP 1.1) File TransportProtocol (FTP)
Network Client Types	Microsoft Windows 95/98/NT 4.0/2000/Me/XP Macintosh Systems OS 8.x, 9.x, X v10.x Sun Solaris 7, 8, 9 HP-UX 11AIX 4.3.3 UnixWare 7.1.1 Red Hat Linux 6.2, 7.2

Feature	Specification
Server Emulation	Windows 2000 Windows NT 4.0 AppleShare 6.0 NFS 2.0/3.0 DHCP
Network Security	Microsoft Active Directory Service (ADS) Microsoft Dynamic DNS Microsoft Lightweight Directory Access Protocol (LDAP v3) Client Windows Domain Controller UNIX Network Information Service (NIS) File and Folder Access Control List (ACL) Security for Users and Groups Secure Sockets Layer (SSL v3) 128-bit Encryption Secure Shell (SSH)
System Management	Browser-based user interface for remote system administration NASManager utility (platform independent) SNMP (MIB II and Host Resource MIB) User disk space quotas for Windows, UNIX/Linux and Macintosh Group disk quotas for Unix/Linux Environmental monitoring E-mail Alerts
DHCP Support	Supports DHCP for automatic assignment of IP addresses
Java Application Environment	Enables the development of applications based on embedded Java technology
Operating Sound Pressure	The sound pressure level at the operators position according to IEC 60704:1982 is equal or less than 70dB(A).
Agency Certifications	UL, cUL, CE, CB, FCC Class A, C-Tick, Nemko, TuV, BSMI
North American Warranty	Three-year Rapid Exchange

Snap Server 4400 Specifications

Feature	Specification
Network Connection	Autosensing 10/100/1000Base-T, dual RJ-45 network connectors, with support for load-balancing and failover.
Dimensions	Width .....16.7 in (42.5 cm) Depth .....18.4 in (46.8 cm) Height .....1.65 in (4.2 cm), 1U Weight .....20.5 lbs (9.3 kg)
Power	Power Rating: 100-240 VAC, 50-60Hz, autosensing Input Current: 3.6A (RMS) for 115VAC, 1.8A (RMS) for 230VAC Power Consumption: 90W (steady state), 162W (maximum) Heat Dissipation: 307 BTUs/hr
Operating Environment	50° F to 95° F (10° C to 35° C) 15% to 90% humidity (non-condensing) Vibration: .25G at 10-300Hz Random for 120 min max duration Shock: 6 pulses of 33G for up to 2ms Altitude: 0 ft to 8,000 ft (0m to 2,438m)
Non-operating Environment	14° F to 140° F (-10° C to 60° C) 5% to 95% humidity (non-condensing) Vibration: 2G at 5-500Hz for 90 min max duration Altitude: 0 ft to 35,000 ft (0m to 10,668m)

Snap Server 4200/4500 Specifications

Feature	Specification
Network Connection	Autosensing 10/100/1000Base-T, dual RJ-45 network connectors, with support for load-balancing and failover.
Dimensions	Width .....16.8 in (42.7 cm) Depth .....23 in (58.4 cm) Height .....1.66 in (4.2 cm), 1U Weight .....28 lbs (12.7 kg)
Power	Power Rating: 250W, 100-240 VAC, 50-60Hz, Input Current: 3.6A (RMS) for 115VAC, 1.8A (RMS) for 230VAC Power Consumption: 90W (steady state), 162W (maximum) Heat Dissipation: 307 BTUs/hr
Operating Environment	50° F to 95° F (10° C to 35° C) 20% to 80% humidity (non-condensing) Vibration: .25G at 10-300Hz Random for 120 min max duration Shock: 6 pulses of 33G for up to 2ms Altitude: 0 ft to 6,096 ft (0m to 2,000m)
Non-operating Environment	14° F to 149° F (-10° C to 65° C) 5% to 95% humidity (non-condensing) Vibration: 2G at 5-500Hz for 90 min max duration Altitude: 0 ft to 35,000 ft (0m to 10,668m)

Snap Server 14000 Specifications

Feature	Specification
Network Connection	Autosensing 10/100/1000Base-T, dual RJ-45 network connectors, with support for load-balancing and failover.
Dimensions	Width.....17.0 in (43.2 cm) Depth.....23.0 in (58.4 cm) Height.....5.0 in (12.7 cm), 3U Weight.....75.0 lbs (34.1 kg)
Power	Power Rating: 100-240 VAC, 50-60Hz, autosensing Input Current: 5.0A (RMS) for 115VAC, 2.5A (RMS) for 230VAC Power Consumption: 210W (steady state), 300W (maximum)
IT Power Systems	The Snap Server is also designed for IT power systems with phase-to-phase voltage 230 V.
Operating Environment	50° F to 95° F (10° C to 35° C) 15% to 90% humidity (non-condensing) Vibration: .25G at 10-300Hz Random for 120 min max duration Shock: 6 pulses of 33G for up to 2ms Altitude: 0 ft to 8,000 ft (0m to 2,438m)
Non-operating Environment	14° F to 140° F (-10° C to 60° C) 5% to 95% humidity (non-condensing) Vibration: 2G at 5-500Hz for 90 min max duration Altitude: 0 ft to 35,000 ft (0m to 10,668m)

Taiwan Statement

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Safety Precautions

- **Environmental Conditions —** Make sure the physical environment in which the server resides falls within the specifications for your model as described in this chapter.
- **Installing the Server —** During installation, make sure the server is always placed on a surface capable of supporting its weight.
- **Connecting to the Main Power —** Install the server near an easily accessible power source. Make sure the source is the proper voltage for your model. Place the power cord out of the way of traffic; do not place any object over the power cord.

  If the server is taken offline for an extended period, disconnect it from the power source to avoid possible damage from a power surge.
- **Enclosure Openings —** Openings in the enclosure ensure proper airflow and prevent overheating; do not cover these openings. Never place liquids on or near the server to avoid spillage; liquid entering an enclosure opening could cause fire or electrical shock.
- **Cleaning the Server —** Before cleaning the server, be sure to disconnect all cabling. Do not use any liquid or spay cleaning agents to clean the server; use only a damp sheet or cloth.
- **Servicing the Server —** Never open the Snap Server. For safety reasons, the server should only be opened by qualified service personnel.

If one of the following situations arises, do not attempt a remedy; contact Snap Appliance technical support for assistance before proceding:

- The power cord or plug is damaged.
- Liquid has penetrated the server.
- The server has been exposed to moisture.
- The server continues to operate in an unexpected manner even after solutions suggested in the administration guide have been followed.
- The server is dropped or otherwise physically damaged.
- The server has obvious signs of damage.

Appendix B

Third-Party Backup Applications

This appendix describes how to install the following backup agents on the Snap Server from a Linux or a Windows backup host system:

- CA BrightStor ARCServe 2000 v7.0 Workgroup Edition/Advanced Edition
- VERITAS NetBackup DataCenter and BusinesServer v3.4
- VERITAS Backup Exec v8.6
- Legato NetWorker v6.1.1

These backup packages do not support the backup of extended POSIX ACLs. If you use one of these packages, Snap Appliance strongly recommends you create a Snap Server disaster recovery image as described on page 93 before you perform a backup.

Preparing to Install a Third Party Backup Agent

Before performing one of the backup agent installation procedures described in this appendix, make sure you have the following information and tools.

- **Backup and Media server IP addresses —** Most backup agents need to know the IP addresses of the backup and media servers you plan to use with the Snap Server. You will use the Host File Editor screen in the Snap Server's Administration Tool to supply a hostname-to-ipaddress mapping that persists across system reboots.
- **The agent/client files required by your backup software —** Typically, these files are either provided on your backup software's User CD or available for download from the manufacturer's Web site. You will need to copy these files (usually delivered in a compressed format, e.g. as *.zip, *.tgz, or *tar files) to the Snap Server.

- **A secure shell (SSH) client —** To remotely install any backup agent on the Snap Server, you must use have a secure shell (SSH) client installed on a remote workstation. The Snap Appliance SSH implementation is compatible with both SSH1 and SSH2. If you do not already have an SSH client installed, you can download free or low-cost SSH applications from the Internet.

To prepare to install a backup agent, perform the following tasks:

1 **Identify Backup and Media Servers to the Snap Server.**

In the Administration Tool, navigate to the **Maintenance > Host Editor** screen and click **Add**. In the screen that opens, do the following

a Enter the IP address of the backup or media server.

b Enter one or both of the following as required by your backup software:

- Hostname (long form): Enter the fully qualified address for the backup server using the *myserver.mydomain.com* format.
- Hostname (short form): Enter an abbreviated address for the backup server using the *myserver* format.

Click **Save**. The entry appears on the Host Editor screen. Repeat this procedure for each backup and media server you plan to use.

2 **Enable SSH on the Snap Server.**

Navigate to the **System > SSH** screen, and in the Enable SSH pull-down menu, select *Yes*, and then click **Save**. Secure Shell is immediately available.

Caution Leaving SSH enabled is a security risk. Snap Appliance strongly recommends that you disable SSH as soon as you complete the installation procedure.

3 **Create a directory on the Snap Server called *agent*.**

You must create a directory on the Snap Servers to which you will copy the agent files. For purposes of illustration, the procedures described in this appendix assume that this directory is called agent. Navigate to the **Storage > Directories** screen, click **Create Directory**, enter agent, and then click **Continue**.

Tip VERITAS NetBackup users should skip the next step and proceed to their installation instructions on page 158.

4 **Copy the agent/backup files to the Snap Server.**

Using a method appropriate to your environment, copy the agent/client files to the directory you just created for this purpose.

General Guidelines

Before proceeding with your installation, make note of the following:

- **The Snap Server Backup and Restore Path —** Backup servers often request the path for backup and restore operations on the Snap Server. When you configure a backup server to see the agent or client running on the Snap Server, use the following path:

  /shares/*sharename*

  where *sharename* is the name of the share to be backed up. If you have accepted the default Snap Server configuration, this path is:

  /shares/SHARE1

- **Backup software sees the Snap Server as a UNIX/Linux client —** When you configure a backup server to see the agent or client running on the Snap Server, assume that the server is a UNIX or Linux client.
- **Commands in SSH to the Snap Server are case sensitive —** The commands you must enter via SSH to install your backup agent are case sensitive; pay careful attention to the capitalization of commands, and enter them exactly as shown.

Installing Third-Party Agent Software

For purposes of illustration, the procedures in this section assume that: (1) you are using the default Snap Server configuration; and, (2) you have created a directory called `agent` (to which to copy your agent/client files) on the default share (`SHARE1`), such that the path to the directory is `/shares/SHARE1/agent`.

Installing a CA BrightStor ARCserve Agent

This section explains how to install the CA BrightStor ARCServe 2000 v7.0 Workgroup Edition/Advanced Edition.

1. Connect to the Snap Server via SSH.
2. At the prompt, log in as admin, using the password you created for this account during the initial setup of the server.
3. To change to superuser, enter the following command and press Enter.

   ```
   su -
   ```

4. At the prompt, enter the admin user password, and press Enter.
5. To change to the agent directory, type the following command, and press Enter:

   ```
   cd /shares/SHARE1/agent
   ```

6 To unpack the agent files for CA BrightStor ARCServe 2000 v7.0, enter the following commands at the prompt, and press Enter after each one.

Tip When you unpack the agent files, ignore errors regarding the bin group and bin user will appear. These errors will not affect installation or use of the agent.

```
rpm -ivh --nodeps calicens.rpm
rpm -ivh --nodeps uagent.rpm
rpm -ivh --nodeps asagent.rpm
```

7 To change to the agent directory, enter the following command and press Enter:

```
cd /opt/uagent
```

8 To start the agent, enter the following command and press Enter.

```
./uagentsetup
```

The BrightStorARCserve agent is now installed.

9 Close the SSH client, then return to the Administration Tool and do the following:

a To disable SSH on the Snap Server, navigate to the **System > SSH** screen, select *No*, and then click **OK**. SSH is immediately disabled.

b To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Reboot** screen, and click **Reboot**.

10 Delete the agent files you copied to the to the Snap Server, as they are no longer needed.

11 To verify the success of the installation, use your backup management software to configure and run a test backup.

Installing a VERITAS Backup Exec Agent

To install the VERITAS Backup Exec UNIX/Linux agent, use the following procedure.

1 Connect to the Snap Server via SSH, and log in as admin using your admin user password.

2 To change to superuser, enter the following command and press Enter.

```
su -
```

3 At the prompt, enter the admin user password, and press Enter.

4 To change to the agent directory, enter the following command, and press Enter.

```
cd /shares/SHARE1/agent
```

5 To unpack the agent files, enter the following command, and press Enter.

```
tar vxf filename.tar
```

where *filename* is the name of agent file. Then press Enter to list the files and directories that you are installing.

6 To run the Backup Exec agent installation, type the following command:

```
./INSTALL
```

Then press Enter and follow the prompts, using the default install locations and default options.

Caution You must respond to "yes" or "no" prompts in lower case (y or n); using uppercase will cause an error and abort the procedure.

7 When prompted for the platform, enter n and press Enter to reject the default selection, then specify the Linux 2.4 Kernel (usually option 7), and press Enter.

8 If the script requests the path for backup and restore on the Snap Server, use the following path (assuming you used the default configuration):

```
/shares/SHARE1
```

9 At the multi-NIC machine prompt, enter y and press Enter. Then at the specify network interface prompt, do one of the following:

- If your Snap Server is configured in Standalone mode (multi-homing), enter y, press Enter, then at next prompt, enter the IP address of appropriate port, and press Enter.
- If your Snap Server is not configured in Standalone mode, enter n, and press Enter.

10 Answer the remaining prompts.

11 To start the agent, type the following command and press Enter.

```
/etc/rc.d/init.d/agent.init start
```

The VERITAS Backup Exec agent is now installed.

12 Close the SSH client, then return to the Administration Tool and do the following:

a To disable SSH on the Snap Server, navigate to the **System > SSH** screen, select *No*, and then click **OK**. SSH is immediately disabled.

b To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Reboot** screen, and click **Reboot**.

13 Delete the agent files you copied to the to the Snap Server, as they are no longer needed.

14 To verify the success of the installation, use your backup management software to configure and run a test backup.

Installing a VERITAS NetBackup Client

This section describes how to install the UNIX/Linux agent from VERITAS NetBackup.

1. Copy the NetBackup *NBClients* directory and the *Linux* directory from the root of the NetBackup CD to the *agent* directory on the Snap Server.
2. Connect to the Snap Server via SSH, and log in as admin using your admin user password.
3. To change to superuser, enter the following command and press Enter.

   ```
   su -
   ```

4. At the prompt, enter the admin user password, and press Enter.
5. To change to the agent directory, enter the following command, and press Enter:

   ```
   cd /shares/SHARE1/agent
   ```

6. To run the client installation, type the following command:

   ```
   ./NBClients/catalog/anb/client.inst
   ```

   Press Enter and follow the prompts on the screen.
7. Choose Linux as the OS and press Enter.

   Tip At the end of the installation process, a few errors will appear saying that the installer cannot find the CD-ROM. This is caused by the installer attempting to unpackage the Java files. The required Java files are already on the Snap Server and are not a required component of the installation.

   The VERITAS NetBackup client is now installed.
8. Close the SSH client, then return to the Administration Tool and do the following:
   a. To disable SSH on the Snap Server, navigate to the **System > SSH** screen, select *No*, and then click **OK**. SSH is immediately disabled.
   b. To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Reboot** screen, and click **Reboot**. In the future, the NetBackup Client will start each time you reboot the Snap Server.
9. Delete the *NBClients* and *Linux* directories that you copied from the CD to the Snap Server, as they are no longer needed.
10. To verify the success of the installation, use your backup management software to configure and run a test backup.

Installing a Legato NetWorker Client

This section describes how to install the Legato NetWorker UNIX/Linux client.

1. Connect to the Snap Server via SSH, and log in as admin using your admin user password.
2. To change to superuser, enter the following command and press Enter.

   ```
   su -
   ```

3. At the prompt, enter the admin user password, and press Enter.
4. Use the **cd** command to change to the directory in the share, for example:

   ```
   cd /shares/SHARE1/agent
   ```

5. To unpackage the client files, enter the following commands:

   ```
   tar xvfz nw_linux86.tar.gz
   cd LGTOclnt
   rpm -ivh --nodeps lgtoclnt-x.x-x.i386.rpm
   ```

   where *x.x-x* is the version number.

6. To start the Legato NetWorker daemon, enter the following command at the console:

   ```
   /etc/rc.d/init.d/networker start
   ```

   The NetWorker client is now installed.

7. Close the SSH client, then return to the Administration Tool and do the following:
   a. To disable SSH on the Snap Server, navigate to the **System > SSH** screen, select *No*, and then click **OK**. SSH is immediately disabled.
   b. To start the newly installed backup agent, navigate to the **Maintenance > Shutdown/Reboot** screen, and click **Reboot**.
8. Delete the client files you copied to the to the Snap Server, as they are no longer needed.
9. To verify the success of the installation, use your backup management software to configure and run a test backup.

Backup & Restore Operations with a Legato NetWorker Client

This section describes special procedures Legato NetWorker users must use in order to perform backup and restore operations on the Snap Server.

To Add the Snap Server as a Root User

For backup operations, NetWorker requires that the Snap Server be configured as a root user. To add the Snap Server root user as one of the administrators, use the following procedure.

1. Open the NetWorker Administrator application.
2. Click the **Set Up Server** icon,
3. In the Administrator field, enter

   root@*hostname*,

   where *hostname* is the host name of the Snap Server.
4. Click **OK**.

Recover and Retrieve Operations

The Legato NetWorker administrative interface does not support data recovery operations from a remote client for a Linux-based operating system such as the GuardianOS. To recover data, you must execute one of the following CLI commands from an SSH client.

- **Recover —** The recover command restores data from a normal backup job.
- **Nsrretrieve —** The retrieve command restores data from an archive.

Use either the recover or the retrieve command exactly as described below. For more details on these commands, see the *Legato Networker Command Reference*.

To Recover Data from a Normal Backup Operation

1. Using an SSH client, connect to the Snap Server and log in using the admin user name and password.
2. To change to superuser, enter the following command and press Enter.

   su -
3. At the prompt, enter the admin user password, and press Enter.

4 Enter one of the following commands, then press Enter:

- If recovering data *to its original location*:

  recover -s *backupservername* **-c** *snapservername* **-f -i "/shares/***SHARE1/data/***" -a**

  where **/shares/***SHARE1/Data/* is the path of the data you are restoring.

- If recovering data *to a different location*:

  recover -s *backupservername* **-c** *snapservername* **-f -i -a R -d "/shares/***SHARE1/relocated_data/***" "/shares/***SHARE1/Data/***"**

  where **/shares/***SHARE1/relocated_data/"* is the path to the new target location for the restore operation; and where **/shares/***SHARE1/Data/* is the path of the data you are restoring.

To Retrieve Data from an Archival Backup Operation

1 Using an SSH client, connect to the Snap Server and log in using the admin user name and password.

2 To change to superuser, enter the following command and press Enter.

su -

3 At the prompt, enter the admin user password, and press Enter.

4 Enter one of the following commands, then press Enter:

- If retrieving data *to its original location*:

  nsrretrieve -f -i -s *backupservername* **-A** *annotation* **"/shares/***SHARE1/data/***"**

  where **/shares/***SHARE1/data/* is the path of the data you are restoring.

- If retrieving data *to different location*:

  nsrretrieve -f -iR -d "/shares/*SHARE1/new_dir"* **-s** *backupservername* **-A** *"annotation"* **"/shares/***SHARE1/Data/***"**

  where **/shares/***SHARE1/new_dir"* is the path to the new target location for the restore operation; where *annotation* is the name of the Legato backup; and, **"/shares/***SHARE1/Data/* is the path of the data you are restoring.

Appendix C

Upgrading Backup Express for Jukebox Support

Jukebox (robotic tape library) support enables unattended, lights-out backup operations. Upgrade packages that offer various levels of Jukebox support are available from the Snap Appliance Web site (http://www.snapappliance.com). When you purchase an upgrade, you receive a Proof of Purchase (PoP) number. The PoP number is used to obtain a license key that enables functions in your software. This license key is all you need to activate the upgrade on a Snap Server; no additional software installation is required.

Obtaining the license key

Once you receive the PoP number, use the following procedure to activate the upgrade. Make sure you have a valid server number on hand as well.

1. Go to Snap Appliance's Web site (http://www.snapappliance.com).
2. If you haven't already done so, register your server.

   Your registration record lets you generate license keys to unlock features of Backup Express, and also records the keys you have purchased in case you need to reference them.
3. Using the PoP number and the Snap Server server number, acquire a new license key for the Backup Express for GuardianOS product.
4. On the Snap Server, navigate to the **Maintenance > Feature Licensing** screen and enter the new key.
5. Click **Save**. The new features become active next time you use Backup Express.

Upgrade Notes

The Backup Express for GuardianOS manuals are in PDF format and are in the manuals subdirectory on the Backup Express for GuardianOS User CD-ROM.

You can find the instructions for setting up automated tape libraries for use with Backup Express for GuardianOS in the Backup Express Jukebox Setup Guide (bexjuke.pdf).

If further assistance is required, contact Backup Express Technical Support at (201) 930-8280.

Glossary

Term	Definition
Access Permissions	A rule associated with a share, a file, or a directory to regulate which users can have access to the share and in what manner.
ACL (access control list)	Access control lists control access to directories and files. Each list includes a set of access control entries, which contain the meta data that the system uses to determine access parameters for specified users and groups.
Active Directory Service	Active Directory is the preferred authentication method for Windows XP, Windows 2000, and Windows 2000 Advanced Server network users. This authentication allows Active Directory users to connect to shares on the Snap Server. The Snap Server supports the Microsoft Windows 2000 family of servers that run in native Active Directory Services (ADS) mode or in mixed NT/ADS mode.
Administration Tool	A Web-based utility for the configuration and ongoing maintenance, such as monitoring server conditions, configuring e-mail alerts for key events or for SNMP management.
ADS (active directory service)	A directory service from Microsoft that is part of Windows 2000.
AFP (AppleTalk filing protocol)	A local-area network (LAN) architecture built into all Apple Macintosh computers.
Agent	A program that performs some information gathering or processing task in the background. Snap Servers support a number of backup agents, and can be configured as an SNMP agent.
Algorithm	A sequence of steps designed to solve a problem or execute a process.

Term	Definition
AllLocalUsers group	The AllLocalUsers Group is the default group for all users on Snap Servers. Local users are set up by the Snap Server administrator. Network users or Windows Domain users are not part of the AllLocalUsers group.
AllUsers group	The AllUsers Group is a collection of all users. The Snap Server automatically maintains the AllUsers group.
Array	A series of objects all of which are the same size and type. In a server context, an array refers to the grouping of hard drives into a RAID Set.
Authentication	Authentication validates a user's identity by requiring the user to provide a registered login name and corresponding password.
Autonegotiation	An Ethernet feature that automatically negotiates the fastest Ethernet speed and duplex setting between a port and a hub or switch. This is the default setting and is recommended.
Autosensing	An Ethernet feature that automatically senses the current Ethernet speed setting.
Backup Express for GuardianOS	A comprehensive backup solution that is preinstalled on Snap Servers to support backup and restore operations to a local tape drive.
Bonding	Network bonding technology treats two ports as a single channel, with the network using one IP address for the server. Snap Servers support load balancing and failover bonding modes.
Catalog	A Backup Express for GuardianOS file stored on the Snap Server that keeps track of the data you back up.
Chaining	A native Snap Server technology in which all Snapshots of a volume depend on successive Snapshots for part of their content.
Channel	A communications path between two computers or devices.
Checksum	The result of adding a group of data items that are used for checking the group. The data items can be either numerals or other character strings treated as numerals during the checksum calculation. The checksum value verifies that communication between two devices is successful.
CIFS (common Internet file system)	A specification for an Internet file access protocol that complements HTTP and FTP and reduces access time.
Daemon	A process that runs in the background.

Term	Definition
Default gateway	The network address of the gateway is the hardware or software that bridges the gap between two otherwise unroutable networks. It allows data to be transferred among computers that are on different subnets.
Degraded	A RAID state caused by the failure or removal of a disk drive.
DHCP (dynamic host configuration protocol)	Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses on a computer network. Each system that connects to the Internet/intranet needs a unique IP address. The Snap Server can be configured to perform as a DHCP server and assign IP addresses with a single subnet.
Directory	A virtual folder used to organize files. Also called a folder.
Disaster Recovery	A strategy that allows a company to return to normal activities after a catastrophic interruption. Through failover to a parallel system or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.
Disk	A rigid platter, usually constructed of aluminum or mylar, with a magnetic surface that allows the recording of data, that is stored inside the drive.
DNS (domain name server)	The server that maintains a mapping of all host names and IP addresses. Normally this mapping is maintained by the system administrator, but some servers support dynamic mappings.
Domain	In Windows NT and Windows 2000, a domain is a set of network resources such as users and groups of users. A domain may also include multiple servers on the network. To gain access to these network resources, the user logs in to the domain.
Domain name	The ASCII name that identifies the domain for a group of computers within a network.

Term	Definition
Ethernet	Ethernet is the most widely-installed local area network technology. The most commonly installed Ethernet systems are called 10Base-T and provide transmission speeds up to 10 megabits per second (Mbps). Fast Ethernet or 100Base-T provides transmission speeds up to 100 Mbps and is typically used for LAN backbone systems, supporting workstations with 10Base-T cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 Mbps (one Gigabit or one billion bits per second).
Ethernet address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet port.
Ethernet port	The Ethernet Port houses the network card to provide Ethernet access to the computer.
e*Trust Inoculate*IT	Antivirus software bundled with the Snap Server.
Event	Any significant occurrence in the system that may require notifying a system administrator or adding an entry to a log.
Failover	Failover is a strategy that enables one Ethernet port to assume the role of another port if the first port fails. If a port fails on a Snap Server, the second port assumes its network identity (if the two Ethernet cards have been configured for failover). When the port comes back online, the original identities are restored. Failover is only possible in a dual-Ethernet configuration.
FTP (file transfer protocol)	File Transfer Protocol (FTP), a standard Internet protocol, is a way to exchange files between computers on the Internet. By default, a Snap Server is set up to be an FTP server.
Full duplex	Indicates each communicating systems can each transmit and receive data simultaneously.
Gateway	The network address of the gateway is the hardware or software that bridges the gap between two network subnets. It allows data to be transferred among computers that are on different subnets.
GID (group identification)	Each group on a Snap Server has a unique ID for security purposes.
GuardianOSImage	Image file used to upgrade the GuardianOS.
Half duplex	Indicates one-way transfer of data at a specified speed.
Hidden share	A share that restricts the display of the share via the Windows (SMB), Web View (HTTP/HTTPS), and AppleTalk (AFP) protocols.

Term	Definition
Host name	The unique name by which a computer is known on a network. It is used to identify the computer in electronic information interchange.
Hot spare	A hot spare is a disk drive that can automatically replace a damaged drive in a RAID 1 or 5. If one disk drive in a RAID fails, or is not operating properly, the RAID automatically uses the hot spare to rebuild itself without administrator intervention.
Hot-swapping	The ability to remove and add disk drives to a system without the need to power-down or interrupt client access to file systems.
HTTPS	The HTTP protocol using a Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.
I/O (input/output)	Describes the operation of transferring data to or from a computer, typically through an interface protocol like CIFS, NFS or HTTP. The Snap Server presents a file system to the user and handles block I/O internally to a RAID array.
IP (address internet protocol address)	The unique 32-bit value that identifies the location of the server. This address consists of a network address, optional subnetwork address, and host address. It displays as four addresses ranging from 1 to 255 separated by periods.
Jukebox	A robotic tape backup device that stores numerous tape drives and uses a mechanical arm to bring the drive to a station for reading and writing.
JVM (java virtual machine)	Software that converts Java bytecode into machine language and executes it. A JVM allows an application such as NASManager written in Java to run on any operating system.
Kerberos	Kerberos is a secure method for authenticating a request for a service in a network. Kerberos lets a user request an encrypted “ticket” from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network. In Windows 2000/XP, the domain controller is the Kerberos server. The Kerberos key distribution center (KDC) and the origin of group policies are applied to the domain.

Term	Definition
LCD (liquid crystal display)	An electronic device that uses liquid crystal to display messages on the Snap Server 14000.
LED (light emitting diode)	An electronic device that lights up when electricity is passed through it used on the Snap Server 4400 as status lights.
Linux	The GuardianOS is based on the Linux OS, a UNIX-like OS that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems.
Load balancing	Load balancing is only available in dual-Ethernet configurations. The Ethernet port transmission load is distributed among two network ports (assuming the cards are configured for load balancing). An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses.
Local group/local user	A local user is one defined locally on a Snap Server using the Administration Tool. The local user is defined by the server administrator. Windows Domain, ADS, and NIS users are not considered local.
MAC (media access control)	In the Open Systems Interconnection (OSI) model of communication, the Media Access Control layer is one of two sublayers of the Data Link Control layer and is concerned with sharing the physical connection to the network among several computers. Each Ethernet port has a unique MAC address. Snap Servers with dual-Ethernet ports can respond to a request with either port and have two unique MAC addresses.
Maintenance mode	A series of HTML screens that allow you to perform repair, upgrade, or reinstall the GuardianOS in a disaster recovery situation.
Master server	A server that contains the Backup Express product, including the catalog and modules that control media management, scheduling and distributed processing.
MIB (management information base)	A MIB is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of the SNMP.
Mirroring	RAID 1 uses mirroring, which stores data on one disk and copies it to a second disk, creating a redundant storage solution. RAID 1 is the most secure method of storing mission-critical data.

Term	Definition
Mounted	Describes a file system that is available.
Multi-homed	Describes a Snap Server that is connected to two or more networks or has two or more network addresses.
NAS (network attached storage)	Hard disk storage that is set up with its own network address as opposed to being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The NAS device is attached to a local area network (typically an Ethernet network) and assigned an IP address.
NASManager	A java-based utility for discovering and monitoring Snap Servers.
NFS (network file system)	A client/server application that allows a computer user to view and optionally store and update files on a remote computer as though they were on the user's own computer. The user's system needs to have an NFS client and the other computer needs the NFS server. The Snap Server is configured as an NFS server by default.
NIS (network information system)	A network naming and administration system for smaller networks that was developed by Sun Microsystems. NIS+ is a later version that provides additional security and other facilities. The Snap Server accepts NIS users and groups.
Node	Any device, including servers, workstations, or tape devices, that are connected to a network; also the point where devices are connected.
Orphan	A disk drive that has becomes disconnected from its RAID either by accidental removal of the drive or the intermittent failure of the drive.
Parity	Parity is error correction data. RAID 5 stores equal portions of each file on each disk and distributes parity information for each file across all disks in the group. This distributed parity allows the system to recover from a single disk drive failure.
PoP	Proof of Purchase number used to obtain a license key for an upgrade for the Backup Express for GuardianOS software.

Term	Definition
POSIX (portable operating system interface)	A set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to develop programs that could run on multiple platforms without the need to recode. The Snap Server uses Extended POSIX ACLs.
Protocol	A standardized set of rules that specifies the format, timing, sequencing, and/or error checking for data transmissions.
Public access share	A share that allows all users read/write access to the file system.
Quota	A limit on the amount of storage space on a volume that a specific user or group can consume. The GuardianOS allows you to set quotas for NIS groups and any known user.
RAID (redundant array of independent drives)	A collection of hard drives that act together as a single storage system. Different RAID types provide different levels of data protection.
Recurring Snapshot	A Snapshot that runs at an administrator-specified time and interval.
restrict anonymous	Windows has a feature where anonymous users can list domain user names and enumerate share names. Microsoft has provided a a mechanism in the Registry called restrict anonymous for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. The implementation of the restrict anonymous mechanism may prevent the Snap Server from obtaining the list of account names it needs to authenticate Windows domain users.
Resynchronization	A RAID state which describes the process of integrating a new drive into the RAID.
Rollback	A Snapshot feature that allows the administrator to restore a volume to a previous state as archived in a Snapshot without resorting to tape.
SCSI (small computer system interface)	A parallel interface standard used to attach peripheral devices, such as robotic libraries, to computers.
Serial number	The 10-character alphanumeric number assigned by the manufacturer at the factory.

Term	Definition
Server number	A numeric derived from the MAC address of your Snap Server's primary Ethernet port that is used to uniquely identify a Snap Server.
Server-to-Server Synchronization (S2S)	A SnapExtension that copies the contents of a share from one Snap Appliance server to another share on one or more different Snap Servers. S2S is designed to work with Snap Servers and other Snap Server Storage Solutions.
Share	A virtual folder that maps to the root of a volume or a directory on the volume. Permissions are assigned to a share that determine access for specific users and groups. The share point is the name of the top-level directory of the shared folder.
Share access	Network protocols and permissions granted or denied to users and groups that control user and group access to the files.
SMB (server message block)	A protocol for Windows clients. SMB uses the TCP/IP protocol. It is viewed as a complement to the existing Internet application protocols such as the File Transfer Protocol (FTP) and the HyperText Transfer Protocol (HTTP). With SMB, you can access local server files, obtain read/write privileges to local server files, share files with other clients, and restore connections automatically if the network fails.
SnapDRImage	Snap Server disaster recovery image that saves server-specific settings such as server name, network, RAID, volume and share configuration, local user and group lists, and Snapshot schedules.
SnapExtension	A SnapExtension is a Java application that extends a Snap Server's functionality. SnapExtensions are produced both by Snap Appliance and third-party vendors.
Snapshot	A consistent, stable, point-in-time image of a volume (file system) used for backup purposes.
Snapshot pool	Disk space reserved within a RAID for the storage of Snapshots.
Snapshot share	A virtual folder that allows access to all current Snapshots at the same directory level as the original share on which it is based.

Term	Definition
SNMP (simple network management protocol	A system to monitor and manage network devices such as computers, routers, bridges, and hubs. SNMP views a network as a collection of cooperating, communicating devices, consisting of managers and agents.
SSH (secure shell)	A service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet, but more secure, providing strong encryption so that no passwords cross the network in clear text.
SSL (secure sockets layer)	A technology that provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.
Standalone	A network bonding mode in which treats each port as a separate interface. This configuration should only be used in multi-homed environments in which network storage resources must reside on two separate subnets.
Static IP address	An IP address defined by the system administrator rather than by an automated system, such as DHCP. The Snap Server allows administrators to use DHCP-assigned or statically assigned IP addresses.
Striping	A RAID storage technique that distributes data evenly among all disks in the array.
Subnet mask	A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.
TCP/IP	Transmission Control Protocol/Internet Protocol. A commonly-used networking protocol that supports the interconnection of different network operating systems.
Trap	A signal from the Snap Server informing an SNMP management program that an event has occurred.
U	A standard unit of measure for designating the height in computer enclosures and rack cabinets. One U equals 1.75 inches. For example, the 3U Snap Server 14000 chassis is 5.25 inches high.
UID (group identification)	Each user on a Snap Server has a unique ID for security purposes.
Unassigned	The state of a disk drive that is seated in a bay but has not been incorporated into a RAID.

Term	Definition
UNC (Universal Naming Convention)	In a network, the UNC is a way to identify a shared file in a computer without having to specify (or know) the storage device it is on. In the Windows OS, the UNC name format is as follows: *\\server_name\share_name\path\file_name*
UPS (uninterrupted power supply)	A UPS device allows your computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges. A UPS device contains a battery that starts when the device senses a loss of power from the primary source.
URL (universal resource locator)	Web address.
Volume	A logical partition of a RAID's storage space that contains a file system.
Web View	The Web-browser screen that opens when users access a Snap Server using their Web browsers, and displays a list of all shares.
Windows Domain Authentication	Windows-based networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain. The domain controller can also generate encrypted challenges to test the validity of user credentials. Other systems use encrypted challenges to respond to CIFS/SMB clients that request access to a share.
WINS (windows internet naming service)	The WINS server locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.
Workgroup	A collection of computers that are grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.

Index

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W